DERECHO E INFORMATICA

Hacia el inicio de un NUEVO MILENIO

Ponencias
VII Congreso Iberoamericano
de Derecho e Informática

Del 24 al 29 de abril de 2000
Lima, Perú

115842

UNIVERSIDAD
BIBLIOTECA
DE LIMA

Impreso en los Talleres Editoriales y Gráficos de Editora Perú
Av. Alfonso Ugarte 873, Lima - Perú
Hecho el Depósito Legal Nº: 1501012000-1189

94234

VII CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA

Universidad de Lima, 24 al 29 de Abril del 2000

COMITE ORGANIZADOR

Dr. Pedro Patrón Bedoya
Presidente

Dr. Julio Núñez Ponce
Vice-Presidente

Dr. Carlos Torres y Torres Lara
Miembro Emérito Extraordinario

GRUPO DE APOYO AL COMITE ORGANIZADOR

Dr. Carlos Ferreyros Soto

Dr. José Espinoza Céspedes

Dr. José Ochoa Reyes

Dr. Aldo Elliot Segura

Dr. César Salazar Vera

Dra. Carmen Velarde Koechlin

Dra. Rosario Rodríguez-Cadilla Ponce

Ing. Felipe Sacio Caballero

Sr. Erick Iriarte Ahon

Sra. Martha Díaz Mormontoy

Dra. Karla Martínez Beltrán

Srta. Katitza Rodríguez Perea

Srta. Pamela Navarro Castaño

PRESENTACION

El VII Congreso Iberoamericano de Derecho e Informática : Al Inicio de un Nuevo Milenio a celebrarse del 24 al 29 de Abril de 2000 en la Universidad de Lima, reune a los más distinguidos especialistas de la materia. Desde el primer Congreso Iberoamericano de Derecho e Informática en Santo Domingo (1984) el segundo en Guatemala (1989), el tercero en Mérida, España (1992), el cuarto en Bariloche, Argentina (1994), el quinto en La Habana, Cuba (1996), el sexto en Montevideo, Uruguay (1998), el alto nivel de los ponentes y expositores han caracterizado estos eventos.

El Séptimo Congreso Iberoamericano de Derecho e Informática organizado por la Universidad de Lima , auspiciado por la Federación Iberoamericana de Derecho e Informática (FIADI) , Telefónica y Colegio de Abogados de Lima ha sido oficializado por el Ministerio de Justicia y publicado en papel con la participación de Editora Perú y en publicación electrónica en CD con el sistema Folio, con el auspicio de la empresa PRC Consulting S.R.L. . Los seis temas que se incluyen y que son materia del Congreso tratan los aspectos de mayor actualidad en la relación de la Informática y el Derecho y estos son: Tema1: Derecho e Internet en el Nuevo Milenio. Tema2 : Nuevos Desafíos al Derecho Informatico en el Nuevo Milenio. Temas3: Nuevos Enfoques de la Informática Jurídica y Sistemas aplicados al Derecho. Tema 4: Modernización del Estado, Derecho e Informática. Tema 5: Derecho Empresarial Corporativo e Informatica en el Nuevo Milenio, en el cual se incluye un tema de actualidad la aplicación de tecnología y Derecho mediante la microforma digital. Tema 6: Universidad, Derecho e Informática.

Las ponencias contenidas en el presente volumen constituyen un aporte al Derecho Informático y a la Informática Jurídica, contiene las ponencias presentadas en el plazo señalado en la convocatoria del evento. Será materia de otro volumen las ponencias llegadas con posterioridad.

EL COMITE ORGANIZADOR

Oficializan el VII Congreso Iberoamericano de Derecho e Informática, a realizarse en la ciudad de Lima

RESOLUCION MINISTERIAL

Nº 073-2000-JUS

Lima, 28 de febrero del 2000

CONSIDERANDO:

Que mediante Carta S/N de fecha 28 de enero del 2000, la Comisión Organizadora del VII Congreso Iberoamericano de Derecho e Informática de la Facultad de Derecho de la Universidad de Lima, solicita la oficialización del citado Congreso, a realizarse en la ciudad de Lima del 24 al 29 de abril próximo;

Que durante el desarrollo del mencionado evento se reunirá a los más destacados y reconocidos especialistas nacionales e internacionales de Derecho e Informática, con la finalidad de contribuir al análisis de diversos temas vinculados a esta importante rama del Derecho;

Que el Ministerio de Justicia tiene entre sus funciones sistematizar la legislación y promover su estudio y difusión;

De conformidad con lo dispuesto en el inciso h) del Artículo 6º del Decreto Ley Nº 25993 - Ley Orgánica del Sector Justicia, modificado por la Tercera Disposición Final de la Ley Nº 26612; inciso i) del Artículo 3º, e incisos i) y j) del Artículo 80º del Reglamento de Organización y Funciones del Ministerio de Justicia, aprobado mediante Resolución Ministerial Nº 0190-99-JUS;

SE RESUELVE:

Artículo 1º.- DAR CARACTER OFICIAL al VII Congreso Iberoamericano de Derecho e Informática, a realizarse del 24 al 29 de abril del 2000 en la ciudad de Lima.

Artículo 2º.- La presente Resolución no irrogará gasto alguno al Pliego Presupuestal del Ministerio de Justicia.

Regístrese, comuníquese y publíquese.

ALBERTO BUSTAMANTE BELAUNDE
Ministro de Justicia

INDICE

Pag.

TEMA 1: DERECHO E INTERNET EN EL NUEVO MILENIO

1. Derechos de Autor y Nombres de Dominio en la Era Internet: Una Visión Crítica 11
Emilio Suñé Llinás (España)

2. "Nombres de dominio (DNS), en Internet" 31
Carlos Barriuso Ruiz (España)

3. Pornografía, Racismo e Internet 48
Ezequiel M. Zabale y Guillermo Beltramone (Argentina)

4. El Derecho Telemático: Respuesta a la Convergencia Tecnologica 54
Carlos E. Delpiazzo (Uruguay)

5. "Contenidos y Censura en Internet. Críticas al Proyecto de Ley de Chile, de agosto de 1999" 60
Renato Javier Jijena Leiva (Chile)

6. El Riesgo u Oportunidad del MP3 67
Fredrick Vega Lozada (Puerto Rico)

7. "Dominios y Marcas en Internet. El Reglamento del NIC.CL" 72
Renato Javier Jijena Leiva (Chile)

8. Sistema de los Nombres de Dominio en Chile 76
Humberto Carrasco Blanc (Chile)

9. Figuras Delictivo-Informáticos tipificadas en Chile 85
Marcelo Huerta Miranda (Chile)

10. Los delitos de Hacking en sus diversas manifestaciones 100
Claudio Líbano Manzur (Chile)

11. ¿Nombres de dominio, marcas o no?" 108
Beatriz Rodríguez Acosta. (Uruguay)

12. El contrato de publicidad en Internet 115
Carmen Milagros Velarde Koechlin (Perú)

13. Participación política: de la participación presencial a la virtual (la manifestación a través de Internet) 119
José Vicente Cebrián / José Luis González Quirós (España)

14. El Delito Informático, Ley 19.223 en Chile, VIII Región, Región del Bío – Bío. 130
Angelo Benvenuto Vera (Chile)

15. Conflictos de Leyes y de Jurisdicción en el Cyberespacio: una tesis de trabajo desde la perspectiva del Derecho Internacional Privado Español 144
Marina Vargas Gómez-Urrutia (España)

16. Informe Nombres de Dominio 162
Erick Iriarte Ahon (Perú)

17. Los Delitos Informáticos en el Ciberespacio en la Legislación Peruana 181
Julio Núñez Ponce. (Perú)

Tema 2: NUEVOS DESAFIOS AL DERECHO INFORMATICO AL NUEVO MILENIO

1. La Nueva Ley Española de Protección de Datos de Carácter Personal 191
Valentín Carrascosa López (España)

2. La Protección del Derecho a la Intimidad y Privacidad frente a las Nuevas Tecnologías 213
Aldo Antonio Elliot Segura (Perú)

3. "La influencia de la informática en la actividad probatoria y su regulación en Uruguay" 219
María José Viega Rodríguez (Uruguay)

4. "E-Commerce y Derecho. Una visión sistemática" 228
Renato Javier Jijena Leiva (Chile)

5. Comercio Electrónico, Estado y Derecho 233
Renato Javier Jijena Leiva (Chile)

6. Contratos Informáticos 237
Catherine Ivette Mantilla Sánchez (Perú)

7. Información y Derecho: el Desafío de su Integración 246
Patricia Reyes Olmedo (Chile)

8. Los servicios de certificación 252
Ignacio Alamillo / María Pérez (España)

9. Firma Digital y Proveedores de Servicios de certificación. 266
Renato Javier Jijena Leiva (Chile)

10. "Sobre la no Protección de la Intimidad en Chile. Análisis de la Ley 19.628, de agosto de 1999" 274
Renato Javier Jijena Leiva (Chile)

11. Aproximaciones para una Propuesta Legal en Materia de Medidas Seguridad Aplicable a la Contratación Electrónica en el Perú 282
José Francisco Espinoza Céspedes (Perú)

12. La Libertad Informática: Derecho Fundamental en la Constitución Venezolana 288
Miriam Álvarez B. de Bozo / Flor María Ávila Hernández / Héctor Ramón Peñaranda Quintero (Venezuela)

13. Contratación electrónica, comercio electrónico, firma digital: Planteamientos y alternativas de solución 299
Vania Vergara Lau / Luis Quiñones Olivo (Perú)

14. La Responsabilidad en el marco de la Actividad Informática 304
Gladys Stella Rodríguez (Venezuela)

15. "Respuesta del Derecho Positivo Peruano al Reto de la Fe Pública en Materia Informática" 315
José Ochoa Reyes (Perú)

16. Obligaciones Pactadas Mediante Medios Informáticos 324
Aída Noblia (Uruguay)

17. Habeas Data y Protección de Datos en Latinoamérica. Propuestas de reglamentación y armonización de estándares de protección de datos 339
Pablo A. Palazzi (Argentina)

18. La Firma Digital y la Autoridad Certificante en Uruguay 346
María José Viega Rodríguez (Uruguay)

19. El comercio electrónico: ¿hacia una nueva revolución económica y jurídica? 352
Pedro Juez Martel (España)

20. Globalizacion e Informática Jurídica: El Desafío del Notariado 361
Carlos Ferreyros Soto (Perú)

21. El Impacto de la Era Digital en el Derecho 369
Cristian L. Calderón Rodríguez (Perú)

22. Nombres de Dominio y Derecho Problemática y Líneas Evolutivas 373
Marcelo Bauzá Reilly (Uruguay)

Tema 3: NUEVOS ENFOQUES DE LA INFORMATICA JURIDICA Y DE LOS SISTEMAS APLICADOS AL DERECHO EN EL NUEVO MILENIO

1. El Sistema Costarricense de Información Jurídica 391
Carmen Quesada Chacón / Christian Hess Araya (Costa Rica)

2. La formación de la ley, las Bibliotecas Parlamentarias y las Nuevas Tecnologías 398
Rodrigo Obrador Castro / Patricia Reyes (Chile)

3. Reflexiones sobre el Real Decreto 994/1999 y la Seguridad en Bases de Datos 403
Emilio Del Peso / Mario G. Piattini / Eduardo Fernández-Medina (España)

Tema 4: MODERNIZACION DEL ESTADO, DERECHO E INFORMATICA

1. Orientaciones para la introducción de tecnologías de la información en el Poder Judicial 417
Héctor Mario Chayer (Costa Rica)

2. "Do Estado: uma análise de sua evolução e o papel inevitável da informática em seu processo de adequação aos tempos atuais" 427
Carmen de Carvalho e Souza (Brasil)

3. Informatización jurídica del Poder Judicial. 430
Christian Hess Araya (Costa Rica)

4. Hacia una Democracia Digital: Propuestas de Aplicación 437
Carmen Milagros Velarde Koechlin (Perú)

5. Razionalización Informática para la Legislación. A propósito del Manual del Digesto Jurídico Argentino 442
Antonio A. Martino (Italia)

6. Estudio sobre la Viabilidad Jurídica de un Sistema de Transmisión Telemática de Documentos Administrativos entre Administraciones Públicas 447
Beatriz Verdera Izquierdo (España)

7. El Consejo General del Poder Judicial y la homologación y compatibilidad de los sistemas informáticos en España. 463
Francisco Monterde Ferrer (España)

Tema 5: DERECHO EMPRESARIAL Y CORPORATIVO E INFORMATICA EN EL NUEVO MILENIO

1. La influencia de la Internet en el Marco Regulatorio de las Fusiones y Adquisiciones Corporativas, en los Estados Unidos de América y en México. 473
Juan Antonio Rangel Charles (México)

2. Derecho Empresarial Informático en Internet y el uso de la Microforma Digital 486
Julio Núñez Ponce (Perú)

3. Comercio Electrónico, Consideraciones en Torno a una Nueva Area de Trabajo en Materia Fiscal 495
Italo Fernández Origgi (Perú)

4. Internet en el contexto del Comercio Internacional y las Pautas de Tributación en el Impuesto a las Ganancias Argentino 510
Juan P. McEwan (Argentina)

5. Aplicación de Tecnología y Derecho como un caso de Negocios Telefónica Servicios Digitales 523
Richard Wadsworth Delgado (Perú)

Tema 6: UNIVERSIDAD DERECHO E INFORMATICA

1. La Informática Jurídica aplicada en la Universidad Externado de Colombia 529
Teresa Vargas Osorno (Colombia)

2. Enseñanza de la Informática y la Computación en las Facultades de Derecho. Nuestra experiencia en la UAI. 542
Ezequiel M. Zabale / Guillermo Beltramone (Argentina)

3. Fundamentos para la Autonomía del Derecho Informático en la República Argentina 550
Gustavo A. de Cara Corra (Argentina)

4. Enseñanza del Derecho Informático y del Derecho Informatizado en un Programa de Enseñanzas no Regladas de la UNED 556
Francisco Eugenio Díaz / Araceli Oliver (España)

Programa VII Congreso Iberoamericano de Derecho e Informática **569**

Tema 1

DERECHO E INTERNET EN EL NUEVO MILENIO

Derechos de Autor y Nombres de Dominio en la Era Internet: Una Visión Crítica

Emilio Suñé Llinás (España)
Profesor Titular de la Facultad de Derecho
Universidad Complutense de Madrid
Director del Master en Informática y Derecho

Presentaré la Ponencia que me ha sido encomendada por la Organización de este Congreso Iberoamericano de Informática y Derecho, que se celebra en la Universidad de Lima en el emblemático año 2000, con una sistemática de quince proposiciones o enunciados, los cuales serán convenientemente desarrollados y en los que expongo las razones fundamentales de mi crítica al vigente sistema de derechos de autor sobre creaciones digitales, así como en relación con los nombres de dominio y la organización misma de Internet.

Comoquiera que una sana crítica ha de aportar asimismo soluciones, no me abstengo en absoluto de darlas, antes bien todo lo contrario y ello con la esperanza de contribuir a la apertura de una debate, que a mi juicio es ineludible en la actual textura de la sociedad global de la información.

1.- LA INADECUACION DEL CLASICO SISTEMA DE PROPIEDAD INTELECTUAL, PARA LA PROTECCION JURIDICA DE LOS PROGRAMAS DE ORDENADOR, HA ORIGINADO CONSECUENCIAS QUE CONTRAVIENEN EL DERECHO DE LA COMPETENCIA.

Es un dato, en el Derecho moderno, que la protección jurídica de los programas de ordenador se lleve a cabo a partir de los clásicos esquemas de la propiedad intelectual, es decir, de los derechos de autor, lo que ha dado lugar a más ventajas que inconvenientes, ciertamente, pero la "solución" no deja de estar exenta de estos últimos, que además tienen la suficiente gravedad como para plantearse seriamente la necesidad de acuñar una nueva vía protectora, adecuada no sólo a los programas de ordenador, sino, en general, a las nuevas necesidades y retos que plantea la existencia de la sociedad global de la información. No obstante, cuando se aboga por una nueva vía protectora, como aquí se hace, hay que ser cauteloso, e introducir bastantes matices, porque es lo cierto que hasta el presente, casi todas las excepciones a los criterios generales de la legislación de Propiedad Intelectual, llevadas a cabo en materia de protección del software, han favorecido abiertamente los intereses de las multinacionales del sector, básicamente norteamericanas.

Buena muestra de los inconvenientes del sistema de protección jurídica al uso para los programas de ordenador, se ha puesto de manifiesto en el complejo de casos *United States v. Microsoft*, que contra lo que pudiera parecer no es una "película de buenos y malos"; lo único que sucede es que un sistema inadecuado de protección jurídica del software, convierte al dueño del software de base para PC, en un monarca absoluto, con regalía integral sobre el mercado mundial del software.

Ya se ha dicho que Microsoft no es el malo de la película. Ocurre, simplemente, que una normativa, como la de propiedad intelectual, que nació para regular fenómenos distintos del software, puede provocar, en determinadas circunstancias, situaciones de monopolio que atentan contra el Derecho de la Competencia. Pero entiéndase bien que la principal razón de que se haya producido esta situación no deseable, es que la propia legislación -de Propiedad Intelectual, en este caso- lo hace posible y, en alguna medida, se podría decir que fomenta la existencia de un *status quo* como el actual.

La secuencia cronológica que da origen a los actuales problemas es relativamente antigua, y los primeros episodios litigiosos, son bastante anteriores a la actual disputa entre Microsoft Explorer y Netscape, para el control del mercado mundial de los browser o navegadores web, o la que se asimismo produce entre Microsoft

y Sun Microsystems (propietaria del lenguaje de programación Java, básico para la elaboración de páginas web), por las incompatibilidades que, al parecer, ha generado Microsoft entre el Java standard y el que se emplea en el sistema operativo o plataforma Windows.

Todo se inicia en el año 1980, cuando IBM escoge a Microsoft -empresa fundada por Bill Gates y Paul Allen en 1975- para desarrollar un sistema operativo para el IBM-PC. IBM, que en aquel momento controlaba alrededor del 60% del mercado mundial de la informática, desarrolló su *Personal Computer*, sin ser ni mucho menos consciente de su gran futuro comercial, que en aquellos momentos parecía reservado a los grandes sistemas (hardware y software) *propietarios* de determinada marca. Tan es así que IBM ni siquiera se preocupó de proteger adecuadamente su PC y los componentes del mismo bajo el Derecho de la Propiedad Industrial -patentes-. Microsoft, en cambio, sí protegió bajo las leyes de *Copyright* el sistema operativo MS-DOS (Microsoft Disk Operating System), prácticamente idéntico al PC-DOS, que desarrolló para IBM.

Los errores estratégicos de IBM -fáciles de ver a posteriori- y la bendición que la diosa fortuna dispensó a la correcta política de Microsoft, han marcado el desarrollo de la Teleinformática durante quince años, al menos. Una pléyade de ordenadores personales compatibles con el standard IBM y virtualmente iguales -*clónicos*-, comenzó a ser construida tanto en Estados Unidos, como en otros paises, fundamentalmente los llamados *dragones* asiáticos. En síntesis, por cada PC compatible que se vendía, IBM perdía cuota de mercado, mientras que Microsoft generaba más y más ventas -licencias de uso- de su sistema operativo MS-DOS.

En 1983, Microsoft entró de lleno en el software de aplicación, con el lanzamiento de su conocido procesador de textos *Word*, que ha acabado imponiéndose a sus competidores -y principalmente a *Wordperfect*- de igual manera que prácticamente todo el software de aplicación de interés comercial para Microsoft, se ha impuesto igualmente a sus competidores. La cuestión de fondo es muy sencilla: Quien controla el software de base para la herramienta hardware standard, el PC compatible, con la vigente legislación tiene todas las ventajas competitivas necesarias para hacerse también con el software de aplicación.

Conviene aclarar esta diferencia entre *software de base* y *software de aplicación*, que es fundamental para entender todo lo que aquí se expone. El software de base, o software de sistemas, o plataforma -en la amplia, variable y móvil terminología informática-, son programas que controlan las operaciónes más básicas del ordenador. En este software se suele incluir el sistema operativo, el software de comunicaciones, e incluso el administrador de bases de datos. El software de aplicación -que se basa en determinada plataforma o software de base- es el que permite las más variopintas aplicaciones de la Informática (proceso de textos, hoja de cálculo, presentaciones, bases de datos jurídicas, contabilidad, juegos y un largo, casi eterno, etcétera).

En la presente situación de dependencia del software de aplicación del software de base, cuando los estándares introducidos en la informática personal a nivel hardware -PC compatible- han dado a Microsoft el monopolio del núcleo del software de base -ayer el sistema operativo MS-DOS y hoy Windows-, le dan también las herramientas para controlar el resto del software de base y, por supuesto, el software de aplicación de mayor interés comercial, para una compañía de las características de Microsoft.

Las batallas legales que hoy se libran, afectan fundamentalmente al software de base, y más en concreto al software de comunicaciones. Microsoft, que ya es monopolista en sistemas operativos, intenta controlar ahora la gran red global de telecomunicaciones, la red de redes Internet, a partir, sobre todo, de imponer en este contexto a su propio *browser* o navegador *Internet Explorer*. Ello no quiere decir que el gigante del software, no haya actuado de igual manera en el software de aplicación. Como muestra un botón: El anterior predominio de *Wordperfect* entre los procesadores de textos, ha cedido el paso al actual reinado de *Microsoft Word*, que salvo cambios radicales de contexto, es ya irreversible. ¿Quiere ello decir que *MS Word* es mejor que *WP*?. No necesariamente. Sólo sucede que quien contola el software de base en el que ha de desenvolverse *Wordperfect* -es decir, quien controla el sistema operativo, llámese *MS-DOS* o *Windows*-, tiene demasiadas ventajas competitivas, como para no imponer, frente a otro, su propio procesador de textos, que es lo que ha terminado por suceder.

En esta situación, las controversias jurídicas son inevitables y, como antes se decía, vienen de lejos. De

hecho, el monopolio de Microsoft, con su antiguo sistema operativo MS-DOS, fue ya investigado en 1991 por la Comisión Federal de Comercio de Estados Unidos (FTC). La investigación se archivó en 1993; pero el Departamento de Justicia y la Comisión Europea habían iniciado asimismo sus propias indagaciones[1], que asimismo se archivaron, cuando Microsoft se avino a suprimir sus restricciones contractuales a los fabricantes de ordenadores personales, para cerrar el mercado a otros suministradores de software... pero el caso se reabre en 1995, ante los Tribunales USA, en defensa de los intereses de los consumidores. En el mismo año, el Departamento de Justicia impide que Microsoft cumpla su propósito de comprar *Intuit* -empresa productora de un conocido software de aplicación- debido a que el acuerdo podría provocar un encarecimiento del software y disminuir las innovaciones.

Es precisamente en 1995, cuando Microsoft intenta hacerse con el control no sólo de los sistemas operativos, sino de todo el software de base mundial, al lanzar Windows 95 y regalar con él su *browser* de Internet Microsoft Internet Explorer 2, y desbancar así del liderazgo del mercado de navegadores de la Red a Netscape.

En el fondo la apuesta de Microsoft es todavía de mayor calado y por sus actuaciones, parece evidente que su meta es el control de los centros neurálgicos de la Sociedad Global de la Información, que también pasan por ser un agente principal del nuevo y progresivamente desmonopolizado mercado global de las telecomunicaciones, así como de los contenidos multimedia, que circulan por las grandes autopistas de la información. El intento de Microsoft de hacerse con un importante papel entre los grandes operadores de telecomunicaciones, tuvo que ver con la propuesta de poner en órbita una gan red de satétites de telecomunicaciones, a partir de la parte menos peligrosa -los cohetes- del antiguo arsenal nuclear soviético. Esta idea quedó en *stand by*[2]; pero no así la entrada de Microsoft en el mundo de los grandes proveedores de contenidos multimedia, al aliarse con la NBC, entre 1995 y 1996, y fundar MSNBC, con la inicial finalidad de para crear un canal por cable, así como un servicio de noticias on-line. Otros *steps* en el camino de *Microsoft*, por tener un lugar de privilegio entre los proveedores de contenidos, pasa por la compra, en 1997, de WebTV Networks, con la finalidad de ser pionero en la integración de Internet en los aparatos tradicionales de televisión.

En septiembre de 1997 Microsoft, adelantándose a lo que luego será Windows 98, integra ya en Windows 95, la versión 4.0 del navegador Internet Explorer. A partir de ahí estalla una dura batalla legal entre Microsoft y el Departamento de Justicia, que demanda a Microsoft por violación de la transacción a la que se llegó en 1994, pues no en vano, Microsoft obliga a los fabricantes de ordenadores a instalar su navegador Internet Explorer, como condición para poder adquirir licencias de uso del sistema operativo Windows.

La batalla, o mejor dicho, guerra legal, salpicada de consideraciones técnicas instrumentales de finalidades económicas, está servida; y en ella, aunque es indudable para un observador imparcial, que Microsoft persigue consolidar una posición monopolista en el mercado mundial del software, e incluso hacerse con el control de la mayor parte posible de la sociedad global de la información, no por ello deja de tener Microsoft argumentos legales en su favor, pues no en vano esta situación se produce porque así lo permite, e incluso fomenta, la protección legal que a su sistema operativo otorga la legislación de Derechos de Autor o Copyright.

Para los fiscales no es fácil argumentar que un navegador de Internet no pueda introducirse en un sistema operativo, pues un buen software de base requiere de un sistema de comunicaciones adecuado a los tiempos que corren; y en ellos Internet es ya un dato. No está claro que *se regale* Internet Explorer. Otra perspectiva es que Microsoft se limita a complementar su sistema operativo Windows, para hacer de él una plataforma adecuada a la era Internet.

---

[1] El resumen de esta larga guerra legal, compuesta de varias y separadas batallas, puede verse en Internet: http://w3.el-mundo.es/navegante/diario/microsoft/cronomicrosoft.html

[2] Ello no significa que Microsoft se haya mantenido al margen del nuevo gran negocio de las Telecomunicaciones; y así, en junio de 1997, conforme se precisaba en la dirección de Internet citada en la anterior nota al pie, Microsoft invierte 100 millones de dólares (unos 14:000 millones de pesetas) en Comcast Corp., una empresa que podría llevar accesos de alta velocidad on-line a millones de casas por medio de la televisión por cable.

Si la pregunta es ¿dónde están los límites de un sistema operativo?, hay que afirmar con rotundidad que no cabe dar una respuesta terminante a esta cuestión. Es más, no hay mayor razón -técnica- para impedir a Microsoft que incluya un browser de la red en su sistema operativo, que hacer lo propio con un mini procesador de textos -como lo han sido sucesivamente Write o Word Pad- o un programa gráfico del estilo de Paintbrush o Paint. Si en su momento no se interpusieron acciones legales contra Microsoft, por rebasar los hipotéticos límites del software de base o sistema operativo, tampoco hay razón para hacerlo ahora. La única diferencia real que justifica emprender acciones legales serias ahora y no haberlo hecho antes, es que en este momento es ya evidente que Microsoft sigue un camino de monopolista del mercado mundial del software que, repito, está inducido por una legislación de Derechos de Autor que, definitivamente, no sirve, para regular una realidad de *tercera ola*, cual es la que viene dada por los programas de ordenador. El Estado y fases del correspondiente proceso, puede consultarse en Internet[3].

En sentido parecido, se acusa hoy a Microsoft de hacer lo posible para que el binomio Windows/Internet Explorer plantee problemas de compatibilidad con Java, desarrollado por *Sun Microsystems*, que como dice Andrew Shapiro[4], es un lenguaje de programación "independiente de la plataforma que se use". Al tratarse de un standard no propietario y abierto, Java va en camino de convertirse en la lengua franca de la Web, lo que no conviene a Microsoft, que dificulta la compatibilidad con Windows del Java standard, e incluso intenta crear sus propias alternativas a Java, cual es el caso de Windows DNA, que como se decía en el *Wall Street Journal*[5], bajo el sugerente título *Microsoft intenta desestabilizar a Java*, el referido DNA *utiliza la tecnologia Component Object Model, es decir tecnologia tipo modelo por objeto componente, por la cual se pueden combinar componentes o partes de distintos programas de software escritos en cualquier lenguaje de programacion, incluyendo Java.*

Lógicamente existe también una alianza, conocida como *trust Java*, en la que aparte de Sun Microsystems, se integran IBM en el ámbito del hardware, *Oracle* en bases de datos y *Netscape* entre los navegadores de red, alianza cuya fuerza se ha visto potenciada con la adquisición de *Netscape* por AOL, el mayor proveedor de servicios de Internet a nivel mundial. Con la posterior adquisición por parte de AOL del imperio mediático de Ted Turner, los objetivos -incluso declarados- de esta alianza no son muy distintos de los que persigue Microsoft... y es lógico que así sea, cuando es la propia legislación la que crea problemas, en lugar de resolverlos.

Reitero que el problema de fondo no es una película de "buenos y malos", sino cómo corregir una posición de poder absolutamente dominante que previamente el sistema administrativo y legal, sobre todo de EE. UU., permitió a Microsoft. El dueño del software de base tiene no sólo ventajas competitivas sobre otros productores de software de aplicación, que en un mundo donde el tiempo no es ya oro, sino platino, resultan determinantes; pero es que, además, tiene el poder de la incompatibilidad, lo que equivale a un poder de vida y muerte sobre los productos de la competencia. Reitero que mi crítica no se dirige a Microsoft, que sigue sus propias metas y objetivos empresariales, al igual que lo haría cualquier otra empresa bien dirigida -es decir, orientada a ganar dinero- en su situación; sino al contradictorio sistema administrativo, y sobre todo legal, que hace posible que una situación de este tipo se plantee, por cuanto que lo permitido -e incluso favorecido- por la legislación de propiedad intelectual, acaba entrando en colisión con el Derecho de la Competencia.

2.- LA FORMA JURIDICA DEBE RESPONDER A LA REALIDAD SOCIAL, EN MAYOR MEDIDA QUE LA REALIDAD SOCIAL A LA FORMA JURIDICA.

Personalmente tengo clara la anterior situación desde hace mucho tiempo, y por eso la había expuesto en público, antes de que se convirtiese en un tema de candente actualidad, que conceptualmente sigue sin estar planteado de forma no suficientemente diáfana. En concreto, el día 4 de marzo de 1996, en el marco del Vº Congreso Iberoamericano de Informática y Derecho, durante la presentación del libro *Derecho Informático*,

---

[3] http://www.usdoj.gov/atr/cases/ms_index.htm
[4] Shapiro, A: Hard drive on Microsoft. The Nation, 8 de diciembre de 1997.
[5] Wall Street Journal, 24 de septiembre de 1997.

del Catedrático peruano Julio Núñez Ponce, el Profesor y antiguo Decano de la Facultad de Derecho de la Universidad de Montpellier, Michel Vivant, destacó del libro su tratamiento de la protección jurídica del software, lo que viniendo de Vivant es un halago, al tratarse de una de las mayores autoridades mundiales en la materia. Comoquiera que los aspectos científicos de la presentación entraron en este derrotero, hice la siguiente reflexión, que el propio Vivant consideró acertada.

Desde mi punto de vista, en el establecimiento de una protección jurídica para el software, se había operado exactamente al revés de lo que ha sido habitual en la historia de las instituciones jurídicas. Se había partido de un marco jurídico, al que se procuraba amoldar los problemas concretos, en lugar de diseñar un marco jurídico, para responder a las necesidades planteadas por los problemas concretos.

El Derecho, según entiendo, es una ciencia práctica, de ahí que sus instituciones hayan sido decantadas empíricamente, antes de ser formuladas a modo de grandes categorías legislativas y doctrinales. Esto ha sido siempre así; de ahí la gran importancia que tuvo el Derecho Pretorio, en el proceso de formación del Derecho Romano, al tratarse de un Derecho de construcción jurisprudencial, con las miras puestas en la solución del caso concreto, con una filosofía no demasiado distinta del moderno *Common Law*, que no en vano es un Derecho de creación jurisprudencial. Una vez localizados los grandes problemas y decantadas empíricamente las categorías jurídicas, es cuando se procede a darles rigor lógico y formular grandes cuerpos legislativos, como pudo ser el Digesto o Pandectas, para Roma, o más modernamente los grandes códigos, y señaladamente los civiles. De hecho, el Código Civil alemán fue el resultado de lo que el Maestro Villar Palasí llamaría un largo *año sabático*, de supremo esfuerzo logizador de las categorías jurídicas, que vino dado por la Pandectística, que no en vano se apoyó en el filón inagotable de datos, instituciones y sistemas, aportados por el Derecho Romano.

Primero se detectan los problemas de la realidad social y luego se les dan soluciones jurídicas, cada vez más depuradas, desapegadas de la cortedad de miras de lo empírico, para adquirir la perspectiva general de las grandes instituciones jurídicas y de las buenas construcciones doctrinales. Esto ha sido así, en todas los grandes conceptos, como el de *negocio jurídico*, que no en vano es un producto de la Pandectística alemana, y en cualesquiera instituciones del Derecho, entre ellas la *Propiedad Intelectual* y la *Propiedad Industrial*.

Con el software, sin embargo, se ha seguido un proceso inverso, en el que se ha partido de una categoría jurídica a priori, en este caso la Propiedad Intelectual o Derechos de Autor, en lugar de observar los problemas que realmente se plantean, los cuales tienen, ciertamente, concomitancias con los Derechos de Autor, pero a veces debieran primar los aspectos de Propiedad Industrial, y básicamente del Derecho de Patentes , otras, incluso, las cuestiones relevantes están vinculadas al Derecho de la Competencia, etc. Pretender reducir una problemática tan variada y compleja a los estrictos cánones de los Derechos de Autor, supone querer vestir a David con la camisa de Goliat o, aún peor, a Goliat, con la de David, que quedaría jecha jirones. Desde esta perspectiva procederé, acto seguido, a un análisis crítico de la legislación vigente en España sobre protección del software, así como de la más importantes iniciativas adoptadas en el plano de la Unión Europea y en el de las relaciones internacionales y del Derecho Internacional.

3.- ANALISIS CRITICO DE LA NORMATIVA BASICA SOBRE PROPIEDAD INTELECTUAL DEL SOFTWARE, VIGENTE EN ESPAÑA.

La normativa básica vigente en España sobre Propiedad Intelectual en general, y sobre propiedad intelectual del software en particular, está directamente inducida por diversas Directivas europeas y se contiene, sobre todo, en el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual. Con posterioridad al mismo se ha promulgado en nuestro país la Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, que será objeto de consideración en epígrafe aparte.

El artículo 10.1 del T.R. de la Ley de Propiedad Intelectual -en adelante LPI-, define lo que puede ser objeto de propiedad intelectual, de forma semejante acomo se hace en los demás países de nuestro entorno:

Art. 10. Obras y títulos originales.-1. Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:

i) Los programas de ordenador.

El artículo 96 del propio Texto Refundido, da una definición aceptable de programa de ordenador, que es la siguiente:

Art. 96. Objeto de la protección.-1. A los efectos de la presente Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

En el mismo artículo existen otras disposiciones razonables, asimismo relativas a los programas de ordenador, como la exigencia de originalidad, la no protección de las meras ideas, incluidas las que afectan a la forma de presentación del software -interfaces-, la previsión de que la documentación y manuales de un programa están protegidos jurídicamente de la misma forma que el propio programa y se establece la protección de versiones sucesivas de un programa así como de los programas derivados. Igualmente dispone con acierto la LPI que cuando los programas de ordenador formen parte de una patente o un modelo de utilidad, estarán protegidos, además de por la Legislación de Propiedad Intelectual, por la de Propiedad Industrial, cuya norma básica es la Ley 11/1986, de 20 de marzo, de Patentes.

Es asimismo razonable que el artículo de referencia no dispense protección jurídica a los *virus informáticos* y, en general, a los programas creados *con el fin de ocasionar efectos nocivos a un sistema informático.* Hasta ahí, pues, lo razonable. A continuación, *ciencia obliga*, pasaré a referir lo que no es tan razonable.

4.- LA PROHIBICION DE LOS PROGRAMAS COPIADORES O COPIONES, ES INCOMPATIBLE CON EL DERECHO DEL CONSUMIDOR A TENER COPIAS DE SEGURIDAD DE SUS PROGRAMAS.

En el propio enunciado se hace explícito lo absurdo de establecer prohibiciones que afecten a los programas copiadores, popularmente conocidos como *copiones*, como la que figura en el artículo 102 LPI, que considera infracción del derecho de autor el hecho de poner en circulación, o tener con fines comerciales, programas *cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador.* El absurdo es de tal calibre, que la Ley incurre, incluso, en contradicciones internas, pues no en vano su artículo 100.2 admite que la realización de copias de seguridad por los usuarios legítimos de un programa, no puede impedirse por contrato, si tal copia resulta necesaria para su utilización. Comoquiera que muchos programas comerciales disponen de protecciones software, prácticamente el único medio, a la vez sencillo y eficaz de burlar tales protecciones, con el fin legítimo de realizar una copia de seguridad, es utilizar un programa copiador, que, sin embargo, no puede ser comercializado lícitamente, a tenor del artículo 102 LPI. La razón de esta contradicción hay que buscarla en el desmesurado afán del Legislador -que en lo sucesivo aparecerá de forma tan reiterada como constante- de proteger los intereses de los fabricantes de software, por encima de cualquier otra consideración.

La Ley de Patentes, en su propio ámbito -artículo 57-, consigue la finalidad que seguramente aquí se pretende, al establecer que la explotación de una patente no puede llevarse a cabo de forma contraria a las leyes, la moral o el orden público. Sin duda hubiera sido mucho más adecuado establecer una regla análoga, que afectase a la forma de uso, más que a su propia existencia, en el caso de los programas copiadores.

La cuestión de los programas copiadores ya fue planteada en 1995, en el ámbito del Libro Blanco sobre Infraestructura de la Información Nacional (N.I.I.) de la Administración Clinton. La legislación propuesta fracasó en el Congreso de los EE.UU. en gran medida a causa de una fuerte oposición a la propuesta de protección técnica, en la que destacaba la oposición de las bibliotecas, de las industrias de bienes de consumo electrónicos y informática, y de la comunidad de la educación.

Lo realmente sorprendente del caso fue que, a pesar de esta derrota nacional, los EE.UU. continuaron presionando en el frente internacional, demandando la adopción de la medida que no lograron sacar adelante en su propio país, en el Tratado sobre Derecho de Autor de 1996, al que se aludirá más adelante. La propuesta de los EE.UU pretendía declarar ilegales los mecanismos cuyo principal propósito o efecto fuese la acción de eludir -*circumvention*- un sistema de protección técnica, incluso cuando el efecto de la acción de eludir consistiese en hacer copias permitidas por la Ley. En otras palabras, la propuesta de los EE.UU. condenaba inadecuadamente la acción de eludir, y no específicamente la acción de eludir con fines ilegales. Cuestión distinta hubiese sido la propuesta de una legislación específicamente dirigida a impedir la acción de eludir ciertos sistemas de acceso restringido, tales como los sistemas de encriptación que impiden el acceso a la emisión de señales de satélite; pero no era el caso.

Es decididamente sorprendente que lo que Estados Unidos no ha podido conseguir en su propio país, lo traslade a la arena internacional y tenga en la Unión Europea, a través de la incorporación de esta medida a sus Directivas, a la más ardiente defensora de lo que, a fin de cuentas, son los intereses de las grandes multinacionales del software, mayormente americanas.

Esta cuestión tiene, por demás, problemas adicionales, desde el punto y hora que la propuesta que formuló Estados Unidos en la Conferencia de la OMPI de 1996, carecía incluso del requisito de conocimiento de la parte del fabricante: un fabricante puede ser considerado responsable, incluso sin saber que un programa de su autoría puede ser usado para infringir la Ley.

La postura de Estados Unidos es lógica, pues la hiperprotección jurídica del software, no hace sino proteger sus intereses de mayor exportador mundial. El propio Miguel Angel Davara[6] ha empleado, para esta situación , la palabra *colonialismo*, y al igual que yo mismo, lo hace sin acritud. Se trata, sencillamente de llamar a las cosas por su nombre. El propio Vicepresidente Al Gore tiene muy claros los intereses americanos: En el documento sobre la Infraestructura Nacional de Datos[7] (NII), se pronuncia muy claramente sobre la importancia estratégica que tiene para EE. UU., la protección de la industria del software.

No se trata aquí tanto de criticar la postura de Estados Unidos, que a fin de cuentas defiende sus intereses, como el seguidismo de esta política, en ocasiones con ribetes ultramontanos, por parte de la Unión Europea, cuyos intereses debieran permitirle plantear posiciones más equilibradas. Bien es cierto, que donde hay un *déficit democrático*, el poder puede actuar sin responder ante el pueblo. Y eso se nota.

5.- EL DESEQUILIBRIO DE LA PROTECCION JURIDICA DEL SOFTWARE, EN FAVOR DE LOS INTERESES DE LAS GRANDES MULTINACIONALES AMERICANAS: DERECHOS DE LAS PERSONAS JURIDICAS Y RESTRICCIONES PARA LOS TRABAJADORES.

A partir de lo que se acaba de exponer, y siempre en la misma línea de favorecer los intereses de las grandes multinacionales americanas, vemos cómo en la protección del software aparecen continuamente extremos exorbitantes con respecto a la Propiedad Intelectual, e incluso contradictorios con las grandes ideas-fuerza que están presentes en la misma; todo lo cual abona el criterio que aquí se defiende, de proteger los programas de ordenador a partir de una legislación específica que, inspirada en parte en la de Propiedad Intelectual, resuelva, a partir de líneas directrices coherentes, la problemática realmente *sui generis*, que presenta la protección jurídica del software. En concreto, el artículo 97 del Texto Refundido LPI, plantea que *autor* puede serlo una

---

[6] M.A. Davara, Derecho Informático, Ed. Aranzadi, Pamplona, 1998. Pág. 383.

[7] A. Gore, La Infraestructura Nacional de Datos (NII) de los Estados Unidos de América: Agenda para la acción. Trad. R. Fdez. Calvo, en la Revista Novática nº 110, 1994. Pág. 3 ss.

[8] De hecho, el artículo 5 del TR de la LPI es muy restrictivo, a la hora de reconocer, como principio, derechos a las personas jurídicas en resta materia. En concreto, dice:

Autores y otros beneficiarios.-1. Se considera autor a la persona natural que crea alguna obra literaria artística o científica.
2. No obstante de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella.

persona jurídica, lo que es incompatible con la esencia de originalidad de la propiedad intelectual clásica[8] y abona la realidad de que aquí, lo que está en juego, no son tanto los derechos de autor propiamente dichos, como intereses económicos que se protegen pura y simplemente en cuanto tales, a través de una vía que no fue pensada para servir exclusivamente a intereses patrimoniales, sino también a derechos morales[9], que en el caso del software se diluyen como un azucarillo, en un proceloso mar de intereses puramente crematísticos.

En idéntico sentido, el párrafo 4º del propio artículo 97 TR LPI, establece que cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador corresponderán en exclusiva al empresario, salvo pacto en contrario. Si esto no es así en el supuesto más tradicional de una pintura hecha por encargo, por ejemplo, no se entiende muy bien por qué ha de serlo en el caso de un programa de ordenador, salvo que se protejan intereses económicos empresariales, en mucha mayor medida que al propio Derecho de Autor. Ello pone de manifiesto una realidad, y es que en este moderno derecho del capitalismo, en el que se concreta no sólo el Derecho Mercantil, sino la mayor parte del Derecho Privado patrimonial, el Derecho de Autor, con muy pocos retoques, sirve en mayor medida los intereses del capitalismo -y sobre todo de las grandes multinacionales norteamericanas del software-, que el Derecho de Patentes.

Esto es así hasta tal punto que, si bien el régimen de las invenciones laborales se regula de forma muy parecida en el artículo 15.1 de la Ley de Patentes, el apartado 2 del mismo artículo, a diferencia de lo que sucede en la LPI -más favorable, por tanto, a los intereses de la empresa-, matiza que cuando la aportación del trabajador a la invención y la importancia de la misma, excedan de manera evidente del contenido de su relación laboral, el trabajador tendrá, pese a todo, derecho a una remuneración suplementaria por su realización. Por lo demás, hay que decir que la Ley de Patentes tiene una regulación muy completa de las invenciones laborales, en las que se incluyen expresamente las efectuadas por los funcionarios públicos, incluidos los profesores universitarios, por lo que una extensión de dicho régimen a la Propiedad Intelectual del software, hubiese sido lo más adecuado. La verdad es que si se hubiera partido, para la protección del software, del Derecho de Autor, para complementarlo, en aspectos puntuales, con criterios sacados del Derecho de Patentes y el Derecho de la Competencia, se hubiera obtenido una legislación mucho más equilibrada que la actual, en cuyo desequilibrio se halla la razón última de los efectos perversos que produce, de los cuales, la mejor muestra se halla en el caso Microsoft.

Lo que realmente ha sucedido es que el éxito de los Estados Unidos en impulsar a nivel global una legislación, absolutamente desequilibrada, en favor de sus grandes multinacionales del software, en un caso concreto se les ha escapado de las manos. Para los Estados Unidos, la situación ideal en el mercado mundial del software, era la creación de un oligopolio global dominado por empresas americanas; pero la situación se ha desbocado hacia algo que se parece más a un monopolio que a un oligopolio y que afecta a la libre competencia, tanto a nivel global, como en el propio mercado interno de los Estados Unidos.

6.- LA DURACION DE LA PROTECCION JURIDICA DEL SOFTWARE EXCEDE CON MUCHO DE LOS INTERESES A LOS QUE SIRVE.

Esta afinidad del régimen jurídico de la propiedad intelectual del software, con los intereses del núcleo duro del capitalismo; es decir, de las grandes multinacionales americanas, se hace de nuevo evidente en lo relativo a la duración de la protección: El artículo 98 LPI, al inspirarse en criterios propios de la legislación de Propiedad Intelectual, establece unos tiempos que se alejan, con mucho, de la dimensión real de los intereses protegidos, hasta el punto de que si no fuera porque lo establece la Ley, se diría que estamos ante un abuso de derecho, figura que en el fondo consiste en el ejerciciode un derecho subjetivo, más allá del interés objetivamente protegido. No es, pues, abuso de derecho; se trata, simplemente, de derecho desde el abuso.

---

[9] Como es sabido, los derechos morales de autor son, esencialmente, el de paternidad o atribución, que da derecho al reconocimiento de la autoría de la obra, el derecho de decidir sobre su publicación, y el derecho a la integridad de la obra, que puede impedir su modificación por terceros.

No es razonable, dada la velocidad del cambio tecnológico, que un programa de ordenador se proteja en ningún caso más allá de los 20 años -término que ya se plantea con amplitud de criterio-, y que es el criterio establecido en el artículo 49 de la Ley de Patentes, el cual, en buena lógica de valoración de los intereses en juego, es el que debiera haberse trasladado a este supuesto. Dice el artículo 49 de la Ley 11/1986, de 20 de marzo, de Patentes.

La patente tiene una duración de veinte años improrrogables, contados a partir de la fecha de presentación de la solicitud y produce sus efectos desde el día en que se publica la mención de que ha sido concedida.

Pues bien, el precepto realmente aplicable al caso, el referido art. 97 LPI, en el caso de las personas físicas remite esta cuestión a las reglas generales de la Ley, cuyo artículo paradigmático es el 26, que establece que tales derechos duran toda la vida del autor y setenta años después de su muerte. En el supuesto de las personas jurídicas, el artículo 98 dispone que la duración es de setenta años, contados desde el día uno de enero del año siguiente al de la divulgación lícita del programa, o al de su creación, si no se hubiera divulgado. El absurdo presente en esta cuestión es de tal magnitud, que la Propiedad Intelectual, aplicada a los programas de ordenador, que conceptualmente es Derecho Civil, se ha convertido en derecho del capitalismo, en mayor medida que el Derecho de Patentes, que conceptualmente es Derecho Mercantil.

7.- LA PROHIBICION DE LA COPIA DOMESTICA DEL SOFTWARE, ES UNA INJUSTIFICADA EXCEPCION A LOS PRINCIPIOS GENERALES DE LA LEGISLACION DE PROPIEDAD INTELECTUAL.

Otro aspecto digno de comentario es el relativo al contenido de los derechos de explotación, cuyo enfoque es, de nuevo, decididamente desequilibrado, desde el punto de vista de los intereses en juego. Sirve exclusivamente a los intereses de los grandes productores de software y a este efecto, no existe ningún empacho en sobrepasar,a favor de los mismos, las reglas generales de la Legislación de Propiedad Intelectual.

En concreto, *se prohibe la reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria.* En otras palabras, queda prohibida la denominada *copia privada* o *copia doméstica*, autorizada con carácter general por el artículo 31.2 TR LPI, que posibilita la reproducción de obras ya divulgadas, sin autorización del autor, para uso privado del copista, siempre que la copia no sea objeto de utilización colectiva ni lucrativa. Por lo demás, diré que prohibir la reproducción transitoria, tampoco tiene mucho sentido. Si es costumbre en un comercio de artículos fonográficos, la reproducción de la música, antes de decidirse por la adquisición de la correspondiente copia de la obra musical, en el caso de los programas de ordenador, la Ley impone, literalmente, la compra *a ciegas*, al prohibir radicalmente la reproducción transitoria del programa en la menoria RAM del ordenador, imprescindible para poder hacerse una mínima idea acerca de su funcionamiento. No es, en absoluto, razonable, que haya que acudir -en el caso de España, que tiene esta legislación-, a la regulación del período de prueba de un producto y correspondiente plazo de desistimiento, contemplados en el artículo 10 de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, para efectuar una comprobación a posteriori, que debiera poder haberse hecho, aunque fuese mínimamente, antes de comprar el producto.

La cuestión de la prohibición de la copia privada, en el ámbito del software, es más injustificable todavía, si se tiene en cuenta que incluso en el ámbito de las patentes se regula una institución parecida. Así, en el artículo 52 de la Ley de Patentes se precisa que los derechos atribuidos por la patente no se extienden a los actos realizados en el ámbito privado y con fines no comerciales.

Sobre todo la cuestión de la prohibición de la copia privada o doméstica es inconcebible, habida cuenta de que el propio Texto Refundido de la LPI,de 12 de abril de 1996, establece mecanismos -ciertamente muy colectivistas, burocratizados y que claramente persiguen el clientelismo cultural- de remuneración a los autores... que para más inri, no alcanzan al software, puesto que la copia doméstica -que sin embargo se seguirá haciendo y es muy difícilmente perseguible- está excepcionalmente prohibida. En el fondo se está creando una cultura inquisitorial, por la que se pretende que todo consumidor de informática tenga complejo de *pirata informático* -personalmente

no conozco a nadie que haya adquirido el cien por cien de los programas que tiene en su ordenador-, cuando este mismo consumidor tiene, sin el menor complejo, soportes audiovisuales obtenidos mediante grabación casera, que sí son legales al amparo de la razonable normativa sobre copia doméstica, que intenta reducir el concepto de fraude a la explotación comercial no autorizada de la propiedad intelectual de otra persona.

Esta materia, que es la que da lugar al conocido *canon sobre las fotocopiadoras*, se regula de forma compleja en el artículo 25 TR LPI. El derecho se refiere a la reproducción realizada exclusivamente para uso privado, mediante aparatos o instrumentos técnicos no tipográficos, de obras divulgadas en forma de libros o publicaciones que a estos efectos se asimilen reglamentariamente, así como de fonogramas, videogramas o de otros soportes sonoros, visuales o audiovisuales. En concreto se establecen cánones, sobre equipos o aparatos de reproducción de libros, fonogramas y videogramas; así como sobre materiales de reproducción sonora, visual o audiovisual. Según el párrafo 7 del artículo 25, el derecho de remuneración se hará efectivo a través de las entidades de gestión de los derechos de propiedad intelectual, cuyo interlocutor a estos efectos, será el Ministerio de Educación y Cultura.

Nada obstaría a que en el caso del software, se admitiese la copia privada o doméstica, articulándose un sistema de cánones sobre determinados productos informáticos, que incluso podrían distribuirse de una forma no burocratizada, y además absolutamente justa, si se devolviesen bajo forma de deducciones fiscales proporcionales a las ventas declaradas. Esta misma fórmula sería también la más adecuadada para distribuir el *canon sobre fotocopiadoras, cintas de video,* etc., si de verdad se pretende compensar a los autores y no fomentar el clientelismo de las organizaciones que dicen representarlos.

Incluso sería admisible que el cánon sobre los soportes informáticos fuera más alto que los cánones actualmente existentes, pues no deja de ser cierto que en los objetos tradicionales de la propiedad intelectual, el coste de los soportes era proporcionalmente más alto y la dificultad de reproducción mayor que en el caso de los modernos soportes informáticos que, con una gran facilidad y a un coste irrisorio, permiten grabar en ellos tanto software, como los más diversos productos multimedia.

8.- PROHIBIDO TRUCAR UN COCHE.

El artículo 99 b) TR LPI, también prohibe la traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador. Se trata de una disposición insólita, que de nuevo no tiene correspondencia alguna con el más racional Derecho de Patentes, que debiera haberse tomado como modelo, en todo aquello en lo que la protección jurídica del software no tuviera encaje en el ámbito de los derechos de autor.

En otras palabras, cuando la Propiedad Intelectual del software, está especialmente construida desde la perspectiva patrimonial, resulta casi incoherente esta insistencia en la *integridad* de la obra, que como derecho moral, se adapta mejor a objetos tradicionales de propiedad intelectual, que al software. La única explicación razonable es que al tratarse de un derecho pensado desde el estricto punto de vista de los intereses de los productores, prácticamente no establece concesión alguna a los intereses de los consumidores. Otros autores, como Olivier Hance, formulan críticas parecidas, al destacar la extrema dificultad de aplicar el derecho a la integridad de la obra, en el ciberespacio, hasta el punto de que abogan por eliminar el derecho a la integridad, incluso sobre obras más tradicionales que el software, cuando circulan por Internet. Dice Hance:

En Internet los trabajos se modifican constantemente y después se vuelven a enviar o a distribuir, ya sea por su autor original o por otros usuarios, lo cual complica la aplicación de los derechos morales en la red, sobre todo la aplicación del derecho de integridad. En consecuencia, algunos juristas se expresan a favor de una relajación genuina de estos derechos[10].

[10] O. Hance, Leyes y negocios en Internet, ed. Mc Graw & Hill, 1996. Pág. 88.

Mi propuesta es que, en este punto, se apliquen al software las disposiciones del Derecho Industrial, y en este sentido, el ya citado artículo 52 de la Ley de Patentes señala, que los derechos atribuidos por la patente no se extienden a los actos realizados con fines experimentales que se refieran al objeto de la invención patentada. De no existir un precepto así, en el ámbito de las patentes, se daría lugar, por ejemplo, a la prohibición de que terceros efectuasen modificaciones sobre un automóvil de serie, lo que sin duda hubiera abortado el desarrollo de muchos vehículos de altas prestaciones, con el subsiguiente obstáculo para el progreso tecnologico.

Afortunadamente, el artículo 100.1 LPI, introduce mínimos de sensatez en esta cuestión, al precisar que, salvo pacto en contrario, no será precisa la autorización del titular del programa para su reproducción, transformación o corrección de errores, cuando sea necesario para la utilización del programa por parte del usuario, con arreglo a su finalidad propuesta. Asimismo, el artículo 100.5, excluye de autorización del titular del programa, las reproducciones de código y traducciones indispensables, para garantizar la interoperabilidad con otros programas. Incluso en este caso, en la práctica casi siempre surge el problema de que el productor del software tiende a cerrar, en los correspondientes contratos de adhesión, cualesquiera posibilidades que vayan *más allá de lo que estrictamente le exige la Ley.*

9.- CONCLUSION: LA NECESIDAD DE UN DERECHO DE NUEVA PLANTA, MAS QUE SUI GENERIS, ESTABLECIDO SOBRE LA BASE DEL DERECHO DE AUTOR Y COMPLEMENTADO CON PRINCIPIOS Y CRITERIOS EXTRAIDOS DE LA PROPIEDAD INDUSTRIAL Y DEL DERECHO DE LA COMPETENCIA.

Puesto que los hechos son muy tozudos, parece evidente que el camino más correcto para una adecuada protección jurídica del software, pasa por ir a una Legislación de nueva planta que, basándose en la normativa reguladora de los Derechos de Autor, supla sus carencias, con criterios miméticamente recogidos de la legislación de Propiedad Industrial, y sobre todo del Derecho de Patentes, teniendo siempre en cuenta las profundas implicaciones de esta materia, con el Derecho de la Competencia.

Entiéndase bien que no defiendo la creación de un derecho *sui generis*, en el sentido que a esta expresión dan autores como GOLDSTEIN[11], como regulación alternativa tanto a la propiedad intelectual, como a la industrial.

Lo que aquí se propugna es la adopción de una legislación que, partiendo de las bases generales de la regulación de la propiedad intelectual las sustituya, cuando no resulten adecuadas, por criterios procedentes de la propiedad industrial y fundamentalmente del Derecho de Patentes, teniendo siempre presente que esta materia está profundamente entrelazada con el Derecho de la Competencia. En abstracto, probablemente yo también sería partidario del derecho *sui generis*; pero visto lo visto, en el sentido del desequilibrio regulador actualmente existente, en favor de las empresas productoras de software, y fundamentalmente de las grandes multinacionales americanas, acaso sea mejor que cuando la regulación del software deba apartarse de los caminos ordinarios de la propiedad intelectual, intente insertarse, de ser ello posible, en las sendas características de la propiedad industrial. Esta idea no está basada en criterios de estricta oportunidad, sino que la naturaleza del software es, en gran medida, un híbrido entre ambas instituciones. Por una parte es una creación original del intelecto y por otra, al definir el funcionamiento de una máquina, tiene una aplicación práctica, semejante a una invención.

---

11 Paul GOLDSTEIN, Profesor de la Universidad de Stanford, se refiere al futuro de la protección de programas de ordenador en EE. UU. y cita advierte un informe publicado por la Oficina de Valoración Tecnológica del Congreso, qe el que se propone una protección sui generis para los programas de ordenador como una alternativa a formas más tradicionales de protección de la propiedad intelectual e industrial.

Goldstein, P., La Directiva Comunitaria sobre software: una visión desde los Estados Unidos de América, Revista General del Derecho, Febrero de1995.

10.- ESTA CLARA LA GRATUIDAD DEL USO CIENTIFICO E INVESTIGADOR DE LAS BASES DE DATOS; PERO NO LA DEL SOFTWARE QUE LAS GESTIONA.

La protección jurídica de las bases de datos es una cuestión regulada en España recientemente, en concreto por la Ley 5/1998, 6 marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos.

Destaca en dicha Ley (artículo 4.2) el hecho de que establecezcan como gratuitos los usos de las bases de datos, para fines de enseñanza o de investigación científica; por supuesto, siempre que se indique la fuente y que tal uso se lleve a cabo solamente en la medida justificada por el objetivo docente o investigador que se persigue.

Como Profesor de Informática Jurídica, soy especialmente sensible a esta cuestión, que entiendo debiera extenderse a todo el software, y no sólo a las bases de datos, puesto que hoy en día no cabe impartir seriamente docencia sobre cuestiones de Informática Jurídica, que ha de ser necesariamente práctica, sin utilizar programas comerciales de amplia difusión. En otras palabras, no es posible dar una formación razonable en bases de datos jurídicas, sin utilizar las más conocidas, tales como las de La Ley-Actualidad, El Derecho, o Aranzadi, entre otras. De la misma manera, no cabe ningún tipo de formación en Informática Jurídica, ni la inmensa mayoría de las disciplinas relacionadas con la Informática, sin utilizar los programas más habituales, que, en el noventa por ciento de los casos, pasan por la plataforma Windows.

El docente no realiza un uso propiamente dicho del programa o de la base de datos, puesto que dicho uso, en buena lógica, debiera ser el que se produce con arreglo a la finalidad natural del programa, cuya utilidad no es directamente la formación. Es un auténtico abuso -amparado todavía por la Ley en el caso del software-, obligar a las instituciones docentes a adquirir, aunque sea a un precio especial, copias de un programa que no sólo no va a ser utilizado por ellas de forma acorde con su finalidad natural, sino que, a través de la formación de usuarios del mismo, la empresa productora va a obtener, la mayoría de las veces, beneficios indirectos.

La informática moderna, dada su rápida evolución, ha de partir siempre de herramientas comerciales, a las que asimismo debe acoplarse la enseñanza, por lo que a mi juicio es un atentado a la libertad de enseñanza, en las condiciones socio-económicas y tecnológicas en que ésta ha de ser llevada a cabo, que se obligue a las instituciones docentes a adquirir copias de los programas que utilicen exclusivamente para la referida finalidad educativa. Es, pues, encomiable, que esta cuestión haya sido planteada en el caso de las bases de datos, y no tiene excusa que una disposición parecida no se establezca, con carácter general, para cualquier utilización docente del software comercial.

De todas formas, hay que apostillar, que la utilización gratuita de las bases de datos para finalidades docentes e investigadoras, no está del todo clara, pues el artículo 12 LPI, modificado por la Ley 5/1998, distingue claramente entre la base de datos y el software que la gestiona, sujeto a la regulación general de los programas de ordenador. Así por ejemplo, las bases de datos de Aranzadi, están gestionadas por el programa de recuperación de información documental *Knosys*, que es propiedad de la empresa Micronet, las bases de datos de La Ley-Actualidad, por el software *Dataware*, etc.

Teóricamente, las bases de datos de Aranzadi, La Ley-Actualidad..., son de libre uso para finalidades docentes e investigadoras; pero no es igualmente evidente que este libre uso se extienda al software que las gestiona, sin contar con el cual no es posible la utilización de la base de datos. Personalmente entiendo que el espíritu y finalidad del artículo 4.2 de la Ley 5/1998, al permitir la libre utilización de bases de datos para fines de enseñanza e investigación, lleva implícita la libre utilización del software que las gestiona; pero reconozco que la cuestión plantea suficientes dudas como para que no pueda hacerse esta afirmación con total seguridad de que los Tribunales de Justicia vayan a respaldarla, sobre todo cuando, incomprensiblemente, una norma análoga no ha sido establecida para el software en general.

11.- EL DERECHO SUI GENERIS EN LA PROTECCION JURIDICA DE LAS BASES DE DATOS SOLO ES CONSONANTE CON LOS INTERESES DE LAS EMPRESAS PRODUCTORAS.

Por lo demás, en la protección jurídica de las bases de datos, se establece en el artículo 6 de la Ley 5/1998, un derecho "sui generis", que más allá de la protección de las tradicionales vertientes morales o patrimoniales del Derecho de Autor, protege, pura y simplemente la inversión realizada por el productor de la base de datos[12], lo que abona la conclusión, previamente apuntada, de que la problemática global de la protección jurídica del software, se ha planteado sobre la base de los estrictos intereses de los grandes productores de dicho software.

Según el referido artículo 6 de la Ley 5/1998, que modifica el artículo 133 del TR de la LPI, el derecho "sui generis" literalmente significa que el fabricante de la base de datos, puede *prohibir la extracción o reutilización de la totalidad o de una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, siempre que la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo.* El derecho *sui generis* -artículo 136-, se establece para un razonable plazo de 15 años. Por lo demás, terminaré diciendo que la protección jurídica de las bases de datos se articula a partir de los siguientes planos de protección jurídica:

a) Software gestor de la bases de datos, que sigue el régimen jurídico de los programas de ordenador, establecido en la LPI.

b) La bases de datos en cuanto tal, que esencialmente es una *estructura* de los contenidos de la misma, a la que se aplican las reglas generales de la LPI.

c) El derecho *sui generis*, que protege la inversión realizada, al margen de las disposiciones sobre Propiedad Intelectual y que impide, por ejemplo, que se cree una base de datos de estructura original, rellenando sus contenidos, a partir de una copia masiva de datos, procedentes de anteriores bases de datos.

Las excepciones al derecho "sui generis", se establecen en el artículo 135, y se dan en los siguientes casos:

a) Extracciones para fines privados del contenido de una base de datos no electrónica.

b) Cuando se trate de una extracción con fines ilustrativos de enseñanza o de investigación científica, en la medida justificada por el objetivo no comercial que se persiga y siempre que se indique la fuente.

De todo lo anterior se desprende la creación de una barrera, que dificultará el arraigo de nuevos productores de bases de datos, a los que la Ley, de ser aplicada con todo su rigor, prohibiría incluso escanear contenidos que partan de una previa organización de la información en soporte papel. Es de suponer que una consecuencia de todo lo anterior va a ser el mantenimiento de precios caros en las bases de datos, que en lugar de estimular el desarrollo de la sociedad de la información, mediante el empleo de estímulos a la actividad de sus agentes, probablemente consigan el efecto contrario. No me sorprendería que algunos de los actuales suministradores de bases de datos consiguieran, en su momento, entrar en el mercado a través de la captación masiva de datos procedentes de bases de datos de otros productores; y a partir de ahora, están legalmente blindados contra nuevos agentes que quieran utilizar procedimientos incluso más razonables que los que ellos mismos emplearon.

12.- ACTUACIONES RECIENTES EN EL MARCO DE LA OMPI.

En el ámbito internacional, el replanteamiento de la protección jurídica del software, no debiera ser en principio difícil, por cuanto que el tratamiento de los Derechos de Autor y de la Propiedad Industrial, se lleva a cabo, en ambos casos, en el marco de la OMPI (Organización Mundial de la Propiedad Intelectual), cuya crea-

[12] De hecho, hay bases de datos, como las guías profesionales, donde la originalidad brilla por su ausencia.

ción es relativamente reciente, si bien, como es de sobra conocido, hay que buscar sus orígenes remotos en los años 1883 y 1886, cuando se adoptaron el Convenio de París para la Protección de la Propiedad Industrial, firmado el 20 de marzo de 1883, y el Convenio de Berna para la Protección de las Obras Literarias y Artísticas, firmado el 9 de septiembre de 1886.

Ambos Tratados estipulaban la creación de Secretarías que fueron unificadas el 1 de enero de 1893 bajo una misma dirección y conocidas por las siglas BIRPI y, con los años, llegaron a convertirse en la OMPI que fue creada en la Conferencia de Estocolmo por el Convenio de 14 julio de 1967[13], estableciéndose su sede en Ginebra.

En lo que se refiere a la actividad reciente de la OMPI, en el ámbito del Derecho de Autor y de ciertos Derechos Conexos, tras la adopción, en diciembre de 1996, del Tratado sobre Derecho de Autor (WCT) y del Tratado sobre Interpretación o Ejecución y Fonogramas (WPPT), la OMPI se ocupa de la preparación de un Protocolo Audiovisual para complementar el WPPT en lo que respecta al derecho de los artistas, intérpretes o ejecutantes sobre plasmaciones audiovisuales de sus interpretaciones o ejecuciones, así como de un Tratado sobre Bases de Datos, que establezca una protección *sui generis* para las mismas, aunque no reúnan las condiciones necesarias para la protección por la vía del Derecho de Autor.

De todas estas cuestiones, la más importante a nuestros efectos es el Tratado sobre Derecho de Autor de 20 de diciembre de 1996, que estuvo abierto a la firma hasta el 31 de diciembre de 1997, y que se produjo como resultado de la Conferencia Diplomática de la OMPI sobre ciertas cuestiones de Derecho de Autor y Derechos Conexos, celebrada en Ginebra, del 2 al 20 de diciembre de 1996; pero algunos de los problemas más importantes, se plantearon en relación con el Tratado de la misma fecha, sobre Interpretación o Ejecución y Fonogramas, a colación de si las copias temporales en memoria RAM, debían entenderse o no como *reproducción*, a los efectos de la legislación sobre Propiedad Intelectual.

13.- LA ABSURDA PROBLEMATICA DE LAS COPIAS TEMPORALES EN LA ERA INTERNET.

De todas las cuestiones planteadas en el curso de la Conferencia Diplomática, según Jordi Masdevall[14], la propuesta de incluir las copias temporales dentro del derecho de reproducción tenía un serio peligro de frustrar por entero el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas. La importancia de esta cuestión deriva de que difícilmente se puede visualizar cualquier contenido multimedia de una página web, sin previamente reproducirlo en la memoria volátil (RAM) de nuestro ordenador... o sin que previamente se haya reproducido en el servidor de nuestro proveedor de servicios de Internet, por poner sólo algunos ejemplos.

Que tal cosa se plantee como una reproducción no autorizada de un contenido sujeto a la protección de la legislación de Propiedad Intelectual, es tan absurdo como entender que, por la mera lectura en voz alta de una obra literaria, se da lugar a una reproducción no autorizada de la misma, a través de las óndas sónicas, que viajan en el soporte aire. Pues bien, si nadie llega al grado de necedad de entender como reproducción no autorizada, la lectura en voz alta de una obra literaria, tampoco debiera entender como tal la visualización de contenidos multimedia, o la ejecución de programas en la memoria de trabajo (RAM) del ordenador, a condición de no volcarlas en un soporte más estable como un disco... y aun así, no siempre la inclusión de contenidos en disco debiera entenderse como reproducción no autorizada, en un sentido merecedor de protección legal; pues muchas de estas pretendidas "reproducciones" -como las que se realizan en un *proxy*-, no son en realidad sino medios técnicos para optimizar el funcionamiento de la red.

Al final, el artículo 7 del Tratado sobre Interpretación o Ejecución y Fonogramas, se formuló en términos ambiguos, que acto seguido fueron interpretados de forma algo más razonable. Dice el artículo 7 del Tratado:

---

[13] Convenio de la Organización Mundial de la Propiedad Intelectual, de 14 de julio de 1967 (BOE núm. 26, de 30 de enero de 1974).

[14] Jordi Masdevall, Tesina presentada en el III Master en Informática y Derecho, celebrado en la Facultad de Derecho de la Universidad Complutense, Madrid, 1998.

Los artistas intérpretes o ejecutantes gozarán del derecho exclusivo de autorizar la reproducción directa o indirecta de sus interpretaciones o ejecuciones fijadas en fonogramas, por cualquier procedimiento o bajo cualquier forma.

Así expresado, puede entenderse incluido en el derecho de reproducción, el hecho de cargar una imagen, contenida, por ejemplo, en una página web, en memoria RAM; pero la Declaración Concertada relativa a los artículos 7, 11 y 16 de dicho Tratado, está redactada en los siguientes términos:

El derecho de reproducción, según queda establecido en los Artículos 7 y 11, y las excepciones permitidas en virtud de los mismos y del Artículo 16, se aplican plenamente al entorno digital, en particular a la utilización de interpretaciones o ejecuciones y fonogramas en formato digital. Queda entendido que el almacenamiento de una interpretación o ejecución protegida o de un fonograma en forma digital en un medio electrónico constituye una reproducción en el sentido de esos Artículos.

De alguna manera la expresión *almacenamiento* supone, en su sentido más habitual, una cierta *permanencia* de la información, lo que parece excluir la usualmente denominada "reproducción temporal"; si bien hay que reconocer que el actual ámbito del derecho de reproducción, especialmente con respecto a las copias temporales, es poco claro y desde luego se presta a la polémica. De hecho, después de arduas discusiones, al final, lo más que hizo la Conferencia Diplomática fue acordar una declaración sobre el derecho de reproducción que no aludiera la cuestión de la copia temporal. Incluso esta declaración generó disputas y, a diferencia de las demás declaraciones acordadas por la Conferencia, fue adoptada no por consenso, sino por mayoría, después de un debate que subrayó la diversidad de interpretaciones a las que está sujeta.

De hecho, el artículo 7, en su inicial redacción, daba lugar a problemas todavía mayores, que se pusieron de manifiesto durante el debate. Con mucha razón, algunas delegaciones temían que, a menos que fuese debidamente acotado, el artículo 7 podría dar lugar a la obstaculización legal de la actividad de curiosear -*browsing*- y privaría a los proveedores de servicios -tales como acceso a Internet y *backbone providers*- de una mínima seguridad jurídica, que estaría permanentemente amenazada por el riesgo de estar dedicándose sin saberlo a la usurpación de derechos de autor, pues no en vano hacen permanentemente copias temporales de cualesquiera obras puestas en sus sistemas por los usuarios, sobre los que, en nombre de la sacosanta libertad de información, e incluso del más elemental sentido común, no pueden ejercer una actividad inquisitorial. La situación jurídica de los proveedores de servicios en Internet se torna todavía más complicada, habida cuenta de que algunas de estas cuestiones tienen, incluso, repercusiones en un ámbito jurídico tan estructuralmente indisponible como el Derecho Penal.

Las pretensiones de los grandes suministradores de contenidos y de los Estados que más allá de toda lógica les apoyan, entran de lleno en el absurdo, si se constata que cada día los proveedores de servicios transmiten millones de mensajes digitales, y la transmisión de cada mensaje exige siempre al proveedor de servicios hacer varias copias temporales del mismo. Ni es viable controlar todos estos mensajes, ni sería tolerable que se hiciera tal cosa en una sociedad democrática, por lo que el proveedor no puede saber si los artículos transmitidos en su red están o no autorizados. Con iniciativas como las aquí descritas, la moderna ciberinquisición, o inquisición de la copia, está pidiendo con grandes aspavientos que en el cibermundo se rompa el sacrosanto principio de la inviolabilidad de las comunicaciones, por intereses crematísticos que están más allá de cualquier justificación racional y moral.

Incluso habría que decir que en la sociedad global de las telecomunicaciones, la copia adquiere otro carácter que el que tenía en las sociedades de segunda ola, pues forma parte de los hábitos de vida de las sociedades de tercera ola, en un sentido completamente distinto al que protegían los clásicos derechos de autor. Si logra arraigar la inquisición de la copia, tal como hasta ahora se está planteando, la mera consulta de páginas web, que no en vano supone "copiarlas", tal como lo entiende la ciberinquisición, en memoria RAM, podría considerararse ilegal. Por supuesto, serían igualmente ilegales las reexpediciones de mensajes de E-Mail a terceros, y no digamos ya a una lista de correos.

En la última fase de las sociedades de segunda ola, la de la *legislación motorizada*, en afortunada expresión de Forsthoff, habíamos asistido al declinar de la costumbre como fuente del derecho que, a mi juicio, se

situó *de facto* al borde mismo de la desaparición; pero ha sido la propia dinámica social, la que ha acabado convirtiendo en vanos los afanes del legislador, legal o reglamentario, de regular todo lo imaginable. La crisis del Estado es esencialmente una crisis de poder y por lo tanto también una crisis de poder legislativo, por lo que ha de volver a renacer con fuerza el papel de la costumbre[15], la cual, lejos de rendir culto a la tradición, va a ser un mecanismo de autorregulación social, que en el marco de los principios legales, va a hacer posible digerir jurídicamente un cambio tecnológico y por ende social, que circula a tal velocidad, que ha rebasado, incluso, la omnipotencia del viejo *Leviathan*.

En román paladino, esto significa que frente a los problemas artificiales que con un grado extremo de desconocimiento de la realidad tecnológica, se plantean burocratas, legistas de arte menor y demás aprendices de brujo, la sociedad sabe instintivamente distinguir el bien del mal y, en consecuencia, conoce también qué actividades no pueden considerarse como infracciones de la legislación de Propiedad Intelectual, sencillamente, porque son inherentes a la dinámica misma de la información, en su imparable movimiento por el ciberespacio.

14.- LA NUEVA PROBLEMATICA DE LOS DOMINIOS DE INTERNET: NO HAY RAZON PARA QUE NO PUEDAN CONVIVIR CON LAS MARCAS Y NOMBRES COMERCIALES.

Dado el actual volumen, interés comercial y excepcional capacidad de crecimiento de Internet, ha adquirido gran importancia la necesidad de proveerse de *ámbitos reservados de ciberespacio*, que es, a fin de cuentas, lo que nos otorga una identidad en el mismo. Este ámbito -*domain*, en inglés- particular del ciberespacio, es lo que se conoce con el nombre de *dominio* y, a priori, parecería razonable que estuviera en una cierta armonía con determinados sectores del Derecho Industrial, como son los nombres comerciales y, sobre todo, las marcas.

Un dominio es, por ejemplo, *ucm.es* que corresponde a la Universidad Complutense de Madrid, radicada en España. Otro puede ser *microsoft.com* que identifica, con carácer genérico o global a Microsoft. Todos los paises, salvo EE.UU., que representa, por si solo el 50% de la red, tienen su correspondiente identificativo de dos letras. En cambio, las organizaciones americanas utilizan dominios genéricos o globales y algunos estrictamente reservados a los Estados Unidos, como .gov (Administración civil) .mil (Administración militar) o .edu (instituciones educativas).

Los abogados anglosajones ya se refieren a los dominios como las nuevas marcas, y hay una relación comercialmente clara, pero jurídicamente confusa, entre estos dos bienes inmateriales. Para las empresas de hoy, disponer de un dominio que se corresponda con una marca registrada idéntica es esencial y será mucho más importante en el futuro, en la misma medida en que crezca el comercio electrónico. Y lo mismo que se suele decir de las marcas , se podría decir, con mayor razón si cabe, de los nombres comerciales.

La armonía entre dominios, marcas y nombres comerciales, que es lo razonable a priori, resulta a la postre difícil de implementar, debido a la particular organización de Internet, que se produce, fundamentalmente, a través de una autorregulación que opera al margen de los Estados y, en buena y consiguiente medida, del propio Derecho. Aunque no estaría de más plantearse si esta presunta autorregulación es tal y más en concreto si se ha permitido el actual estado de cosas, porque le interesa a algún Estado en particular, que de esta manera puede imponer mejor su peso específico a nivel global, pues de otra manera se vería estrictamente obligado a pactar la organización de la Red de Redes con otros Estados, a través de un Tratado Internacional de alcance

---

15 Sobre la importancia de la costumbre en el ciberespacio, me gustaría destacar lo que dice Olivier Hance, con respecto a los grupos de noticias:
Se considera que quien envía una carta al grupo tiene autorización implícita de reproducirla a todos los miembros del grupo. A la inversa, no existe ninguna autorización implícita, para que envíe esta carta a otros grupos de interés.
O. Hance, Leyes y negocios en Internet, ed. Mc Graw & Hill, 1996. Pág.97.
Otros autores, como Rose, se refieren también a la idea de la autorización implícita, para que desde una página web se establezcan enlaces -links- a la página web de otra persona; aunque los buenos usos exigen notificarle la existencia de tales enlaces.
L. Rose, Netlaw: Your rights in the online world, ed. Osborne Mc Graw & Hill, 1995. Pág. 86.

más o menos universal, que a mi juicio es ineludible para una adecuada regulación de la cuestión. Esta no es, por supuesto, la situación actual.

Resulta a la vez sorprendente, y hasta tedioso, para quien no es un maníaco del intervencionismo y todavía menos un antiamericano, verse forzado a adoptar una posición muy crítica para con la regulación vigente, por la sencilla razón de que es tan absolutamente desequilibrada como injusta. Parece que la única preocupación de esta legislación, sea procurar la sumisión del propio Derecho, a un capitalismo que, por lo que se vé, campa a sus anchas, sin ataduras de ningún tipo, por la aldea global -no sé si habría que decir *zoco global*-. Esta situación acaso resulte grata a los neoliberales; pero es perfectamente detestable -por injusta- para los liberales que lo son, y por eso no necesitan de etiquetas adheridas al nombre de la libertad. Es triste que algo que ya había sido planteado por John Locke, en su 1er. Tratado sobre el Gobierno Civil -la refutación a Filmer-, haya sido sencillamente olvidado en nuestra época.

Volviendo a la cuestión que nos ocupa. El registro de dominios, que acaba de sufrir importantes variaciones, que más adelante veremos, tradicionalmente ha sido coordinado -de forma más nominal que real- por la IANA (*Internet Assigned Number Authority*). No obstante, la competencia para el otorgamiento de dominios está transferida a los NIC (Network Information Center). Los NIC se distribuyen por países, a fin de otorgar los conocidos dominios *.es* (España), *.fr* (Francia), etc. Como dice Daniel David Casla Hidalgo, *como curiosidad hay que señalar que existen dominios de este tipo que no corresponden propiamente a Estados soberanos. Gibraltar, por ejemplo, gestiona su propio dominio bajo las iniciales "gi", y lo mismo ocurre con otras zonas como la Antártida. La causa de esta chocante situación es que en el estándar internacional ISO-3166 que se sigue en el DNS figuran también territorios que no son Estados*[16].

Tradicionalmente han existido, además, los dominios genéricos o globales -aunque en el fondo todos son globales- antes aludidos, algunos de los cuales tienen una enorme importancia comercial. El que más *.com* (entidades mercantiles); pero también *.net* (proveedores de servicios de red) y *.org* (organizaciones sin ánimo de lucro). Sin importancia comercial, tenemos *.int* reservado a las Organizaciones Internacionales. Este último está gestionado por la Unión Internacional de las Telecomunicaciones.

Por lo que se refiere a los demás dominios genéricos que se acaban de citar, tradicionalmente, el enorme poder que comporta el otorgamiento de los mismos lo ha tenido, sobre el pape,l InterNIC; pero en la práctica ha cedido esta importante gestión, ni más ni menos que a una empresa denominada Network Solutions Inc. (NSI). Por cierto, ¿a santo de qué una Internet presuntamente autorregulada ha regalado un negocio de este calibre, durante tanto tiempo, a una sola empresa?. De vuelta a la cuestión que ahora nos ocupa, diré que de los NIC que otorgan los dominios nacionales destaca, a nuestros efectos, ES-NIC, integrado en el Consejo Superior de Investigaciones Científicas.

La asignación tradicional de los dominios se producía a través de reglas internas de cada uno de los NIC, de los que el más importante era, como es lógico, NSI, que operaba, al principio, bajo la máxima *prior in tempore potior in iure*; o si se prefiere la tan coloquial expresión en Inglés, *first come, first served*; pero después cambió -razonablemente- el criterio, en el sentido de proceder a la revocación de aquellos dominios, en los que se certificase la existencia de una marca registrada de cualquier país, que fuese anterior al correspondiente dominio... lo que, como se ha puesto de manifiesto en el caso de Repsol-YPF, es ya insuficiente, pues al parecer el dominio Repsol-ypf.com y la mayoría de sus variantes han sido *ocupados*, o mejor dicho, *okupados*, antes incluso de que se hubiera llevado a cabo la fusión entre dos importantes compañías petroleras; pero cuando ya era bastante obvio que iba a producirse.

Toda esta problemática ha sido generada a partir del pingüe negocio obtenido por muchos de los denominados *cybersquatter* o *ciberokupas*, quienes aparte de conseguir cifras multimillonarias[17] de la venta de do-

---

16 CASLA HIDALGO, D.D.: El sistema de nombres de dominio: Su evolución y los conflictos con el derecho de marcas. Tesina presentada en el IVºMaster en Informática y Derecho, Facultad de Derecho de la Universidad Complutense, Madrid, 1999..

17 El record lo tiene altavista.com, por el que Compaq pagó 530 millones de pesetas, para radicar en él su conocido buscador, según información aparecida en el periódico El País, de 9 de agosto de 1999.

minios, previamente reservados, con mucha perspicacia, tales como consumers.com; en ocasiones han traspasado claramente las barreras de lo ético, al *okupar* denominaciones tales como notarios.com al parecer con el único propósito de venderlas.

Hoy por hoy, existen diferencias de gran calado entre los supuestos regulados por la legislación de marcas -y nombres comerciales, no lo olvidemos- y las nuevas cuestiones que plantean los dominios de Internet, puesto que en el Derecho de Marcas rigen los principios de especialidad y de territorialidad, que son inaplicables a los dominios, en su actual estructura, por lo que, o se cambia la estructura de los dominios en un sentido muy distinto de los cambios que ahora están en curso, o la armonización entre dominios y marcas, no se va a poder llevar a cabo de una manera satisfactoria.

El principio de especialidad significa que las marcas no son universales, sino que protegen concretas categorías de productos y/o servicios, con arreglo a la clasificación que figura en el Acuerdo de Niza de 1957 y que, por supuesto, se recoge en el grupo normativo de la ley 32/1988, de 10 de noviembre, de Marcas, vigente en nuestro país, y en concreto en el artículo 4.4 de la Ley, que dice:

El uso de una marca para un producto o servicio determinado sirve para acreditar tal uso con respecto a productos o servicios de la misma clase del nomenclátor internacional o a productos o servicios similares, o a productos o servicios en relación con los cuales la utilización de la misma marca por un tercero podría dar lugar a riesgo de asociación por los consumidores respecto del origen de unos y otros.

El principio de especialidad es, hoy por hoy, casi por completo extraño a los dominios, pues las distinciones existentes entre las diversas clases de dominios (.com .net etc.) son muy someras. Una armonización futura, que con voluntad de llegar a ella sería posible, probablemente debiera partir de la idea de asimilar la estructura de los dominios, a la de las marcas y los grupos en que éstas se clasifican.

Por lo que se refiere al principio de territorialidad, si bien los dominios pueden asignarse a través de NIC nacionales, no existe inconveniente alguno en solicitar y obtener un dominio global o genérico, que no es más caro que uno nacional. En ocasiones su otorgamiento es incluso más ágil -desde luego en el caso de España esto es así- y, a veces, se establecen reglas tan absurdamente burocráticas que, en España, no se permite el uso del nombre de una Nacionalidad o región, ni siquiera a la Comunidad Autónoma que la representa legítimamente; y ello, irónicamente, porque la normativa privada de ES-NIC ha intentado inspirarse, aunque de una forma harto ultramontana, en el artículo 11.1.c) de la Ley de Marcas, que prohibe utilizar como tales *signos o indicaciones que sirvan en el comercio para designar (...) la procedencia geográfica.*

Así por ejemplo, la Comunidad Autónoma de Aragón ha debido conformarse con aragob.es mientras que Euskadi ha optado por prescindir del .es y registrarse en NSI como euskadi.net, con lo que el Gobierno Vasco, aparte de no tener siquiera ocasión de integrarse en España, al menos en la peculiar interpretación que da el CSIC (ES-NIC) a lo que puede ser y no ser un nombre de dominio, aparece como un proveedor de servicios de red, lo que, obviamente, no es el caso. Aparte de todo lo anterior, en la red de redes, desde un punto de vista estrictamente técnico, todo dominio tiene por definición un alcance global.

En cambio, para las marcas rige plenamente el principio de territorialidad, sobre todo porque sobrepasarlo resulta caro, pues no en vano la denominada marca internacional se configura como un haz de marcas nacionales, lo que resulta paliado pero no estrictamente contradicho en Europa, por el Reglamento del Consejo 40/94, de 20 de diciembre de 1993, sobre la Marca Comunitaria.

Quiero insistir, además, en que la analogía de los dominios está todavía más acentuada con los nombres comerciales que con las marcas, hasta el punto de que probablemente, incluso hoy, podrían ser considerados como tales, desde el punto de vista del Derecho Mercantil. A tal efecto, quiero destacar lo dispuesto en el artículo 78.5 de la Ley de Marcas, cuando dice: *el empleo del nombre comercial como denominación para aplicarse a los productos o servicios en perjuicio de una marca, será considerado, en su caso, como violación del derecho exclusivo de marca o como acto de competencia desleal.*

Conforme puede verse por el dominio notarios.com, las interferencias de los dominios, no se producen sólo con las marcas y nombres comerciales; sino que alcanzan a denominaciones genéricas correspondientes a determinadas instituciones, e incluso pueden afectar a personas físicas, sobre todo famosas. Es posible que empañen, incluso, la honorabilidad de determinadas empresas, como ha sucedido en España con la conocida marca *Nocilla*, fabricante de un producto entre crema y golosina, destinado mayormente al público infantil, bajo cuya denominación existía un dominio de carácter pornográfico, nocilla.com, al que un juez civil de Oviedo pudo obligar al cambio de denominación. En ocasiones, incluso, la confusión puede haber sido provocada, con miras a perpetrar auténticos fraudes, tipificados en el Código Penal.

En general, todos estos litigios se sustancian ante los Tribunales nacionales; pero en ocasiones existen gravísimos problemas, pues nada impediría que el dominio nocilla.com, de carácter pornográfico, estuviese radicado en Perú y sería muy difícil -supongo- convencer a un juez peruano para que prohibiese un uso ofensivo para una empresa española, de la que probablemente los propietarios del dominio, ni siquiera tenían noción de su existencia. Nada impediría tampoco que, mediante testaferros, el referido dominio reemprendiese su actividad en el país más insospechado y la prueba de la conexión entre los anteriores nuevos titulares del dominio, podría resultar poco menos que diabólica.

En la reforma en curso del sistema de nombres de dominio, poco o nada se resuelve
en cuanto a los problemas de fondo, y muy señaladamente en relación con los conflictos que se plantean con las marcas y nombres comerciales. Los cambios, siendo importantes, se han quedado en aspectos más de carácter organizativo, que propiamente sustantivo.

En grandes líneas, el antiguo papel de la IANA (*Internet Assigned Numbers Authority*) -demasiado vinculada a la Administración USA, habría de pasar al ICANN (*Internet Corporation for Assigned Names and Numbers*), que administraría el entero sistema de gestión de nombres de dominio y direcciones IP. Será precisamente el ICANN, el que deberá aprobar los nuevos dominios genéricos que están propuestos desde 1977. Se trata de . *firm* -empresas en general- *.store* -comercio minorista- *.web* -actividades en la red- *.info* -información- *.arts* -cultura- . *rec* -entidades recreativas- . *nom* -personas físicas-.

La previsión de creación de los anteriores nuevos siete dominios de primer nivel, que fue llevada a cabo por el IAHC (*Internet ad hoc Committe),* integrado por Organizaciones Internacionales gubernamentales y no gubernamentales de enorme peso específico en Internet, se vio complementada por la propuesta de desmonopolización del registro de los nombres de dominio globales, hasta ahora llevado a cabo por la empresa NSI, que habría de distribuirse en el marco del CORE (*Council of Registrars*), que al borde del año 2000 ha iniciado su actividad.

Incluso se ha previsto que el CORE solucione posibles controversias entre nombres de dominio y marcas; pero en ningún momento se ha planteado la solución más lógica, que -reitero- se halla en la armonización entre nombres de dominio y marcas registradas, que debería extenderse también a los nombres comerciales y demás nombres y denominaciones, tanto públicos como privados. Se trata de un problema complejo; pero ni mucho menos inabordable.

El sistema CORE, obviamente no gusta a NSI, que ve peligrar su monopolio y -como corresponde a sus intereses- hará todo lo posible por mantenerlo; ni tampoco a los Estados Unidos, que con el nuevo sistema son "algo menos" dueños de la red, por lo que hacen y harán todo lo posible por evitar que se les vaya de las manos.

De hecho, la Administración USA publicó en 1998 un Libro Verde, bajo el título de *Propuesta para mejorar la administración técnica de los nombres y las direcciones de Internet* que , en el mismo año, daría lugar a un Libro Blanco en el que la Administración USA fija su política, con respecto a las propuestas presentadas en el Libro Verde. Básicamente se intenta crear una Entidad distinta del ICANN, para sustituir a la IANA que, por supuesto, tendría su domicilio en los Estados Unidos y, aunque habla de abrir el mercado rel registro de dominios, no está nada claro que de verdad pretenda acabar con el monopolio de NSI.Por el momento, el sistema CORE ha comenzado su andadura, si bien es cierto que el ICANN está domiciliado en Estados Unidos y, en consecuencia, su creación y régimen de funcionamiento ha de atenerse a la legislación USA.

15.- LOS PROBLEMAS GLOBALES, REQUIEREN SOLUCIONES GLOBALES.

El anterior enunciado queda demostrado con el actual gobierno de Internet, que, al estar en manos de empresas y ONGs, sometidas a una fuerte tutela de los Estados Unidos es, de los modelos posibles, el que mejor sirve a los intereses del coloso americano. Lo grave del caso -pues de sorprendente no tiene nada-, es que nadie con influencia -incluida la Unión Europea- discute esta situación, cuando es obvio que Internet requiere de una regulación basada en un Tratado Internacional de ámbito tan universal como sea posible, que lleve al ámbito de lo jurídicamente normado la actual situación de aparente desregulación, que en la práctica supone la consagración y posible perpetuación del poder de los intereses norteamericanos en la red.

La necesidad de reconducir la actual situación a un marco jurídico adecuado, que sólo puede venir del Derecho Internacional Público, aunque las soluciones que éste arbitre puedan ser, muchas veces de Derecho conflictual, se pone también de manifiesto con lo que ha acontecido en algunos litigios en materia de Derechos de Autor, al que se regresa para cerrar el tema. Uno de estos litigios lo cita Duncan Gates en una Tesina presentada en el marco del III Master en Informática y Derecho[18]:

Casos como el Nottinghamshire County Council v. Gwatkin, resuelto el 3 de junio de 1997, ilustran los problemas de utilizar una decisión judicial nacional para impedir determinadas infracciones del derecho de autor, por ejemplo la reproducción ilegal, en el ámbito de Internet.

En el supuesto referido, un informe sobre abusos perpetrados a menores, redactado por los servicios administrativos de una municipalidad británica, fue publicado por tres periodistas ingleses en un dominio de Internet. El ayuntamiento casi inmediatamente logró obtener una orden judicial de la *High Court*, que después de determinar que la actuación de los periodistas infringió las leyes de Copyright, ordenó que el informe fuese retirado de Internet. Sin embargo, copias del informe habían ya aparecido en más de veinte sitios distintos, establecidos como sedes-espejo (*mirror sites*) en servidores de Internet localizados fuera de Inglaterra. El cumplimiento de la resolución judicial, a pesar de la rápida actuación de los Tribunales, era ya prácticamente imposible.

Otro supuesto muy parecido y de mayor repercusión en la opinión pública que el indicado por Duncan Gates, se produjo con la publicación en Internet del libro *Le grand secret*, considerado un libelo en Francia, y en el que Gubbler y Gonod publicaban detalles escabrosos sobre la salud y el pasado político del ex-Presidente Mitterand.

Ello pone de manifiesto que la información es una realidad global, que requiere soluciones globales; pero este es un tema demasiado genérico para ser abordado aquí en toda su extensión, e incluso con una extensión solamente razonable, por lo que lo dejaré para otra -ya que no mejor- ocasión.

---

[18] GATES, D.: Marcas y nombres de dominio. Tesina presentada en el III Master en Informática y Derecho, celebrado en la Facultad de Derecho de la Universidad Complutense, Madrid, 1998.

"Nombres de dominio (DNS), en Internet"

Dr. Carlos Barriuso Ruiz (España)
carlosbar@icam.es

Ilustre Colegio Abogados de Madrid
Madrid, Abril del 2000

1- FUNDAMENTO DNS Y EL COMERCIO ELECTRONICO

Las actuales estrategias de comercio electrónico pasan por posicionarse estratégicamente en la red y el marketing on-line contempla la necesidad de encontrar el dominio adecuado para cada empresa. Al tener un Dominio propio, reforzamos la imagen de la empresa, y defendemos nuestra marca. Además aunque cambiemos de IPS, podremos seguir manteniendo el mismo nombre de dominio.

La identificación de los ordenadores en Internet, incluidos los servidores de Web,s y de correo electrónico, se realiza mediante su dirección IP, pero para facilitar el uso "no amigable" de esta dirección, se crean los nombres de dominio. El DNS (Domain Name Server) es el sistema jerárquico que gestiona los nombres de dominio. Esto se consigue mediante una base de datos distribuida en los servidores de DNS, por los distintos nodos (hosts) de Internet.

De la misma forma que en el comercio tradicional, las marcas y patentes registradas evitan su aprovechamiento ilícito. En el comercio electrónico los dominios equivalen a la marca o nombre en Internet de la empresa, pero teniendo presente que el mercado electrónico tiene un carácter global que aun no esta del todo resuelto.

Desde la perspectiva del IPS, es conveniente admitir la gestión el registro de dominios, pues traerá mas servicios asociados.

El sistema de nombres de dominio (DNS), desarrollado por el ya fallecido Dr. Jonathan B. Postel director de la IANA durante casi treinta años, es clave para Inernet. Sin el no seria posible el funcionamiento correcto del comercio electrónico, del correo electrónico, el direccionamiento de los datos, la petición de recursos, la búsqueda de una web, el uso de FTP, etc.

Al principio el direccionamiento se hacia de forma unívoca con un simple fichero de texto, pero cuando Internet creció (AÑO 1.987), fue necesario implantar el DNS.

En 1969 se crea ARPANET, precursora de Internet, de origen militar. Así se explica que la NSF (National Science Foundation), delegara en NSI que trabajaba para ARPANET y el Pentágono.

Como el crecimiento de los registros de dominios era vertiginoso y los conflictos empezaban a surgir. Surge en 1996 la IANA que junto con la ISOC iniciaron la reestructuración del DNS formando el IAHC (Internacional ad hoc comité) comité que agrupo a las partes interesadas.

El IAHC crea nuevos dominios genéricos y admite a nuevos registradores (el contrato con NSI terminaba el 30 de Septiembre de 1998) y se dota de los siguientes órganos CORE; POC , Policy Oversight Committee, comité de vigilancia para supervisar la transición hacia la primera propuesta de los siete nuevos dominios; PAB (Policy advisory Board). El acuerdo se plasmo en Ginebra el 1-5-1997 en el Memorándum de Entendimiento

EC (Emergent Corporation) se encarga del Diseño y gestión de la nueva base de datos del DNS para los nuevos dominios. (sospechosamente fueron robados los servidores)

Luego EEUU publico su libre verde (30-1-98), rechazado por la Comunidad de Internet. Parecía que la administración EEUU quería perpetuar la jurisdicción de EEUU EN LOS LITIGIOS. Ello determino variar su postura.

2- NOMBRES DE DOMINIO

La estructura de los nombres de dominio, se establece por niveles jerárquicos, de derecha a izquierda y es necesaria para que cada ordenador, en su conexión a Internet, tenga una dirección única con la que se identifica en la red. La distribución del correo postal, se direcciona también sobre una identidad única de todos los domicilios del mundo, el DNS equivale a una guía telefónica de direcciones. El software destinado a la estructuración en el sistema de Nombres de Dominio, en la parte cliente es "Resolver"

Conviene recordar que el acceso a Internet de las grandes organizaciones se hace a través de un router (enrutador) que se convierte en nodo que enlaza con la red troncal del país o con otro de mayor jerarquía, cuyo coste es muy elevado, por ello se utilizan normalmente los servicios de un proveedor de servicio de Internet (ISP) con acceso RTB o RDSI, que nos permite albergar un dominio en un servidor virtual Web, mediante el hospedaje del DNS. Aunque su función principal es suministrar a sus usuarios-clientes una conexión a Internet, mediante el módem conectado a su línea telefónica, hoy ofrecen también servicios de hospedaje (hosting).

3- AUTOREGULACION; ICANN

La autorregulación de Internet, en lo referente a los Dominios, basada en la publicación (5-5-98) del Libro Blanco por la Administración de Estados Unidos y en el consenso Internacional, corrige el pretendido anterior espíritu intervencionista del Libro Verde.

EEUU inicia una transición para retirarse de la gestión de los dominios y de Internet que concluirá el 30-9-2000.

El ICANN (Internet Corporacion for Assigned Names and Numbers) <http://www.icann.org>, Corporación de Internet para la Asignación de Nombres y Números (Nonprofit Public Benefit Corporation) sustituye a la IANA y cuenta entre sus áreas con la especifica de Dominios -DNSO.(Domain Name Supporting Organización), que gestiona los dominios genéricos. Cuyo registro delegara en registradores específicos.

La Unión Europea también propone la autorregulación, incluso la multitud de protestas, habidas en el llamado jueves negro (8-2-96), provocado por la firma de la Ley de Telecomunicaciones por parte del presidente Bill Clinton, marco un antes y después en el pretendido control de Internet.

La IANA (Internet Assigned Number Authority), encarga la gestión del D. territorial a los NIC (España es-.nic: red iris) los genéricos internacionales al NSI compartido con otras muchas empresas repartidas por todo el mundo.

Se firma el "memorándum de entendimiento" GTLD-MOU al que están adheridos ya mas de 250 organizaciones.

4- ASPECTOS LEGALES

La controversia jurídica, de quien esta autorizado para la concesión o no-concesión de un dominio, para decidir la suspensión provisional o definitiva de un dominio, autorizar a un titular u otro frente a un mismo dominio, reasignarlo o simplemente decidir la exclusión del dominio, ha estado siempre flotando en el aire. Naturalmente los Tribunales tienen la ultima palabra. ¿Pero en que país? , ¿En que jurisdicción?, ¿Con que legislación?.

En un principio los nombres de dominio estaban conceptualmente considerados mas una dirección, que una imagen de marca de una empresa como hoy en día se conciben. Del mismo el sistema DNS se asemeja a una guía telefónica de direcciones, con las direcciones de las maquinas.

Por tanto de la propia naturaleza de Internet se infiere su potestad para resolver sobre temas de dominios, como lo hacia la IANA en las discusiones que pudieran crearse. El dominio una vez concedido pertenece a su peticionario.

Pero el comercio electrónico esta haciendo variar este enfoque pues como hemos dicho el nombre de dominio se asocia a la marca de empresa y esta es el valor añadido fundamental de la presencia en Internet.

Los criterios de concesión de dominios corresponden a cada entidad gestora, ya que ellos son los responsables de su dominio. La gestión de dominios territoriales-NIC se delega en organismos con responsabilidad anterior en Internet, en España Csic por su red Iris. No hay pues una autoridad única definida

En los conflictos jurídicos es aplicable el derecho sobre marcas y protección Industrial e Intelectual. La demanda fundamentalmente invocara la acción por utilización indebida sobre marcas.

En la ejecución de la sentencia será cuando se requerirá a la empresa registradora del dominio o el ICANN, aunque ésta, al no tener obligación expresa de acatar la sentencia de otro país, puede crear una inseguridad jurídica que es necesario corregir.

El bien jurídico a proteger es evitar la apropiación y perjuicio de la marca como signo distintivo con gran valor.

Incluso algunas empresas, se dedicaban a acaparar dominios para luego venderlos. Es el caso de la empresa IIS (Internet Information Services). El registro PIZZA.com lo tiene registrado y en venta. La empresa suiza "Bureau d'esprit" tenia 14 dominios como: lemonde.com , cacharel.com.

- "Compaq" llego a pagar entre 3 y 5 millones de dólares por su dominio.
- Por el dominio "Bussines" se pagaron 18 millones de pesetas.
- El nombre "McDonall.com" era de un periodista.
- "Genesis.com", hay una docena de empresas.

También hay quien registra el dominio y luego lo subasta. Por "forgiven.com" se llegaron a pagar 16 millones de pesetas y por el dominio "wallstreet" la empresa Tucson Americana consiguió un millón de dólares en la subasta, el coste inicial de registro fue de 70 $.

Existen países con terminaciones de dominio características, que las venden al mejor postor.

Hoy los tribunales tienden a atajar estas practicas.

La nueva regulacion del Ministerio de Fomento Español tiende a ello lo mismo que, EEUU ha aprobado un reciente "Ley de Prevencion de Ciberpirateria de Marcas , que impida la dilucion de la marca por registro indebido evitando el "ciberquatting" se impondrán sanciones de hasta 100.000$ a los que se lucren indebidamente con estas practicas. No obstante el Gobierno Clinton ha anunciado su oposicion por por ser contraria dice a la libertad de expresion.

La propia Oficina de Patentes y Marcas de EEUU adopto (29-9-99) una Guia de Examen para las Marcas con nombres de dominio identificadores, donde indica norms para rechazarlas.

La propia OMPI (Organización Mundial de la Propiedad Intelectual), ha establecido unas reglas para evitar la especulación.

El NSI, seguía la regla -del primero que solicitaba el dominio en Internet-. Solo suspendía un dominio si se presentaba una reclamación judicial.

No obstante el criterio ha variando desde hace años y así Internic exige al solicitante bajo criterios de buena fe: que esté en posesión pacifica del derecho a usar el nombre de dominio y que no haga uso ilícito o ilegales.

- JURIS Inc. contra Examiner (1996), fue una de las primeras demandas sobre dominios, se resolvió a favor de la tesis de Juris, por tener la marca registrada antes, apreciando la exclusión de otras marcas similares.
- Council of BetterBusiness Bureau Inc versus Mark Sloo que se allano, en el dominio <bbb> .
- Cocacola versus Coca Cola Company el nombre ya había sido registrado.
- Wolkswagen versus Virtual Works que registro en 1996 vw.net por violación de marca , la denuncia se ha interpuesto recientemente (17-10-99) en Virginia sede de vw.
- "Panavision international" versus Denis Toeppen, que registro el dominio Panavision que tenia registrado como marca esta, la sentencia le da satisfacción al titular registral. , 465 U.S. 783 (1984); see also Panavision International, L.P. v. Toeppen, 1996 WL 534083 (C.D. Cal. 1996).
- El Banco Español BBVA le arrebataron la prioridad de inscripcion.
- Compaq pago 530 millones de pesetas para recuperar su dominio "Altavista".
- La corporacion financiera Transasia ha demandado, con poco fundamenteo legal, recientemente (9-3-2000) a la Asociacion Leonardo de las Artes , porque registro ella el nombre de Leonardo , siendo que la asociacion Leonardo publica desde 1968 el Leonardo journal.
- El buscador Ole, perdio su dominio en Argentina (ole.com.ar pertenece a Clarin) y Brasil (ole-.com.br es de Starmedia), dejandoselo asi arrebatar por la competencia.

Así lo normal es que quien tiene un dominio registral y no lo ha reproducido en Internet, si lo hace otro primero tenga que acabar comprándole el dominio, si este ultimo no se allana a la demanda planteada.

El fraude en los dominios ha ocupado un lugar significativo.

- La marca "nocilla" ha consegido que se adopten medidas cautelares por auto de fecha 2-6-99 del juzgado 1ª instancia no. 5 de Oviedo, frente a los registradores en Internet del dominio "nocilla" que ofrecía pornografía. Entre otras contempla el abuso en la propiedad intelectual y el aprovechamiento ilícito del prestigio de una marca.

- El caso del buscador "Ozu" registrado por "advernet" como.es no pide el uso del dominio, sino la oposición a su uso, por otro bajo el nivel .com. Es decir por identidad de marca en otro dominio de primer nivel. Ya que tiene registrado en Internet el primer nivel .es y acciona frente al contrario que tiene registrado el.com. La sentencia de la Juez de BILBAO (VIZCAYA). estimando la demanda interpuesta por ADVERNET S. L., contra D. E. A. R., OZUCOM, S.L. es significativa y condena a estos últimos a :

  - que cesen en los actos que suponen una violación del derecho del titular registral de la marca OZÚ, prohibiéndoles en el futuro la utilización del nombre OZÚ.

  - que no utilicen el dominio Ozu.com (titular Admazing Internet), debiendo quedar revocado el Sr. A. como contacto administrativo.

  - que se cambie la denominación social a fin de que no se produzca confusión alguna.
  - que no utilicen el dominio "ozucom.es".

  - que indemnizen al actor por los daños y perjuicios ocasionados, en ejecución de sentencia.

  - que publiquen fallo de esta resolución en aquellos medios de comunicación que se especifiquen.

Se imponen las costas a la parte demandada.

- Servicios de Telemarketing , S.A. titular registral de sertel contra Serveis Telematics de Balears, S.I. por registrar sertel.es

- Giacalone Versus NetWork Solutions Inc (30-5-96) por el nombre <ty. Com > se resolvió con la compra del dominio por ty Inc.
- El caso de L´oréal contra Vichy.com ordenando su transmision bajo condena de una cantidad por dia de retraso, fue estimado por el Tribunal de Grande Instance de Nanterre 16-9-99. ya que vichy ostenta la proteccion de marca notoria según art. L713-5 del Codigo de la Propiedad Intelectual Frances.

El dominio debe renovarse anualmente, porque de lo contrario se perderá la exclusividad y derechos sobre él y quedara vacante para una nueva solicitud.

Afecta a la propiedad de derechos intelectuales e industriales.

La Jurisdicción y legislación aplicable depende del registrador y territorio.

El arbitraje en la red para solucionar conflictos de dominio es un sistema transparente de autorregulación y es una buena solución siempre que las partes estén de acuerdo en someterse a el.

Si bien por los acuerdos y consensos habidos, para la administración y gestión de los dominios siguiendo un método justo, sistemático y equitativo, se abre la posibilidad de una normativa universalmente aceptada.

El carácter administrativo de Internet no esta muy claro. EEUU, reclama su administración y derechos.
Antes ya la IANA con su comité ad hoc impulsaba ampliar siete nuevos dominios pero el Departamento de Comercio de EEUU, no quiere perder todos los privilegios.

La seguridad Jurídica del comercio electrónico impone, entre otros, llegar a formas efectivas de regulación en el tema de dominios.

Como no existe una normativa definida a nivel Internacional sobre los criterios legales a seguir en orden a determinar la competencia jurisdiccional, lo mas practico es plantear la demanda frente al tribunal que pueda ejecutar la sentencia.

Pero a partir de la descentralización y autorregulación para resolver una demanda sobre propiedad intelectual se podrá optar por la jurisdicción y legislación del país del registrador, del registro o en los EEUU que será lo más efectivo mientras no haya legislación apropiada. Aunque las soluciones extrajudiciales por vía arbitral son más efectivas

Para los dominios territoriales habrá que estar a los requisitos del órgano delegado del NIC y a la legislación estatal del territorio concreto.

Los efectos transnacionales de Internet complican, pues el tema de la Jurisdicción cuando no hay cláusula de sumisión o aceptación de arbitraje. Sobre todo al estar constituida legalmente la ICANN, en EEUU, a diferencia de la IAHC que estaba radicada en Suiza.

5- NUEVO SISTEMA DE DOMINIOS INTERNIC -ICANN

La situación económica del ICANN sucesora de la IANA pasa por dificultades, ya que el Departamento de Comercio del gobierno EEUU, le recomendó que eliminase la comisión de un dólar, que las empresas registradoras le entregaban por cada registro. Ello le ha hecho solicitar ayuda para mantener activa la organización y pensar en redefinir y diseñar, su sistema financiero, de forma definitiva. Algunas empresas se han ofrecido.

El nuevo sistema de dominios de Internet incluye a 87 empresas seleccionadas de todas partes del mundo autorizadas por el ICANN para registrar dominios, en virtud de superar condiciones técnicas y financieras

fijadas y contrastadas por ella, para demostrar su capacidad operativa, que estarán junto a NSI (Network Solutions, Inc.) en régimen de libre competencia, aunque esta ultima conservara temporalmente la gestión de la base de datos de los dominios compartiéndola con otras empresas como por ejemplo:

- Affinity Hosting;
- Alabanza;
- Animus Communications;
- Computer Data Network;
- ComuniTech.Net Inc;
- Concentric Network;
- Domain Registration Services;
- EnetRegistry;
- EnterPrice Multimedia AG;
- GANDI;
- iDirections Inc;
- InterAcces;
- InterNeXt;

6- IDENTIDAD E IDENTIFICACION

Registrar un nombre de Dominio promueve la identidad de la Empresa o de quien lo ostenta como marca, situándolo estratégicamente en todo el mundo.

La seguridad jurídica, en el "comercio electrónico", en orden a la atribución de derechos y obligaciones, exige, estar identificado, causa fundamental para su legitimación como parte. Los dominios (dirección IP) , DNS, etc. es la identidad que nos direcciona al servidor por lo que deben regularse y tener un alto grado de fiabilidad.

Los efectos de los contratos, se delimitan precisamente, a las partes que los otorgan. Si en la contratación analógica, la identificación la componen los nombres y apellidos propios de las personas físicas, inscritos en el registro civil, que en el caso de personas jurídicas será el registro mercantil.

La identificación, como procedimiento para determinar la identidad, se valida mediante la firma y también mediante estampación de signos distintivos.

En la contratación electrónica, la identificación de las partes se hace por el uso de elementos individualizadores y la identificación de los recursos en Internet mediante la dirección URL. Al teclearla va a un srvidor de nombres de dominios que traduce en información digital la dirección IP, con lo cual posibilita localizar la maquina y la información, producto o servicio que se busca.

Pudiéndose establecer criterios de acceso a la información y de autorización para contratar en un determinado sistema.

Pero como en el comercio electrónico, también es necesario identificar los instrumentos interpuestos de hardware y software. En los ordenadores, se determina a través de los nombres DNS o números IP, la dirección del correo electrónico, la clave de acceso a los Host identificados. Completando así, la identificación plena de las partes y del sistema, necesaria para determinar los sujetos de la relación negocial y por tanto de la atribución de sus derechos, deberes y responsabilidades contractuales y extracontractuales.

De hecho, toda auditoría electrónico-informático-jurídica principia con procedimientos exhaustivos de identificación de las partes. Existiendo numerosa normativa que exige la identificación como medio para el ejercicio de acciones.

- El Real Decreto 263/1996, de 16 de febrero, que regula la utilización de las técnicas electrónicas, informáticas y telemáticas (articulando los principios que marca la LRJPAC). Respecto a la comunicación a través de medios electrónicos informáticos y telemáticos señala como requisito de VALIDEZ, la identificación FIDEDIGNA del remitente y del destinatario (art. 7.2). Además de garantizar la transmisión, la emisión, la recepción.
- La Ley 7/1996 de 15 de enero, de Ordenación del Comercio Minorista (*BOE* n.1 15, de 17 de enero, corrección de erratas en BOE n.1 42 de 17 de febrero de 1996), en su artículo 40 (venta a distancia) y artículo 47, indica que la oferta de venta a distancia deberá incluir, entre otros, a) identidad del proveedor, dirección de uno de los establecimientos, domicilio social, documento de desistimiento indicando el nombre y dirección de la persona a quien debe enviarse y los datos de identificación del contrato de los contratantes a que se refiere,
- También la Directiva 97/7 CE (2-5-97) relativa a la Protección de los Consumidores en Materia de Contratos a Distancia, exige con carácter previo a la celebración de cualquier contrato a distancia en su (art. 4), que el consumidor disponga de la información sobre la identidad del proveedor; debiendo esta información según el (art. 5) confirmarse por escrito o por cualquier soporte duradero y expresar la dirección geográfica del establecimiento del proveedor donde el consumidor pueda presentar sus reclamaciones.

Las transacciones en las que no se requiere o no se quiere la identificación como la compra de determinados productos, se efectúan en algunos casos, enviando los mensajes a través de reenvíos anónimos anonymous remailer (ver anonimato).

En favor de preservar la identidad y la intimidad, a ultranza, David Chaum propone el uso de seudónimos distintos para cada tipo de contratación o interlocutores lo que evitaría la posibilidad de definir perfiles en base a datos de un identificador único

La pugna entre la explicitación de datos identificativos y la preceptiva confidencialidad , extensible a la direccion de dominio, se resuelve así con métodos de seguridad, encaminados a evitar la violación del sistema y al mismo tiempo la posibilidad de determinar incuestionablemente la autoría y la autentificación del servidor.

Internet, como soporte de los servicios de telecontratación, pago, y demás actos con transcendencia jurídica. Ademas de contar con la direccion fija o Dominio del comerciante deberia ser conveniente una direccion fija para los usuarios o resto de las partes contratantes.

Esta identificación de los ordenadores es necesaria en Internet como en las redes que usan el protocolo control de transmisión TCP/IP porque la informacion se encapsula y trocea y se direcciona sobre varias topologías, permitiendo conectar redes heterogeneas con diferentes sistemas operativos y distintos formatos de informacion, viajando juntos los datos con el número de identificación y de orden, luego en el destino se recomponen.

La identificación de las partes dentro de X.400 se hace mediante una dirección estandarizada única en todo el mundo. Que se compone de claves de atributos, estructuradas de acuerdo con el protocolo P2 que indican:

- Apellidos y Nombre del titular (S: surname, G: Given Name);
- Nombre de la organización (O: Organización);
- Dominio privado PRMD (P: Dominio de Gestión Privado);
- Dominio de la Administración ADMD (A: Dominio de Gestión de la Administración)
- Nombre del País (C: Country / país)

La naturaleza jurídica de la contratación electrónica impone la necesidad de conocer exactamente de dónde y de quién proviene el documento y su aceptación.

Ademas para acceder o usar los servicios o recursos disponibles, en el comercio electronico, hace falta ubicarlos e identificarlos, así si queremos entrar en un servicio de telecontratación u otros particulares, deberemos facilitar los indicativos correspondientes. Ello se consigue a través del identificador URL.

Cada enlace por donde navegamos en WWW, hasta encontrar la información o servicio deseado tiene una Url asociada.

La URL también indica otros tipos de recursos y servicio distintos a http, como gofher, ftp, etc. Normalizando la forma de especificar la ubicación de cualquier recurso o directorio.

Su nomenclatura representa:

- Primero, el protocolo de transmisión del servidor o recurso deseado, seguido de dos puntos. Ejemplo: El protocolo Http: indica el acceso a WWW, hipertexto. El protocolo ftp: hace ver que queremos acceder a una transferencia de ficheros. El protocolo NNTP que queremos acceder a News: como el servidor de noticias Usenet. El protocolo Telnet, que accedemos a un recurso remoto, donde nuestro ordenador se convierte en terminal del servidor Telnet . El protocolo IRC, accede a una comunicación escrita o verbal, interactivamente y en tiempo real, con uno o varios interlocutores, pública o privadamente.
- Segundo, dos barras de separación seguidas de WWW, sistema Web.
- Tercero, la dirección y ubicación del host servidor, separando por puntos los distintos dominios y separados por / los distintos subdirectorios de acceso hasta llegar al fichero interesado.
- Cuarto, las últimas letras indican de qué tipo son los ficheros, así: Html indica que los ficheros están escritos con lenguaje html; Htm indicaría que los ficheros son del sistema DOS; Gif, indicaría que corresponde a imágenes; etc.

Empleo del dominio en el Correo electronico

Al contratar el mantenimiento del DNS, lo haremos de manera que el dominio se pueda emplear tambien en al correo electronico, no solo en la Web. La dirección de Correo Electrónico estan gestionadas por el proveedor de servicio y son únicas para cada persona en Internet . Se especifican con la norma FQDN, así: consta en primer término del nombre del usuario (asignado por el centro servidor de correo electrónico) que puede coincidir con el nombre real, en segundo término una arroba, en tercer término el nombre asignado al ordenador, y nombre de dominio. Puede emplearse en la dirección de correo electrónico, la dirección IP, detrás de la arroba del proveedor del servicio.

El no indicar estos datos normalmente produce el rechazo del mensaje por remitente desconocido, pero usando centros anónimos la dirección del remitente es borrada y se transforma en no significativa, y si no se especifican más señas, la comunicación es anónima, lo cual es posible por la particularidad de estos centros re-expedidores anónimos.

Que en caso de litigio podrían, si residen en el mismo país, ser emplazados judicialmente para que revelasen la identidad del remitente.

7- DOMINIOS (DNS)

Los ordenadores conectados a las redes tienen una identificación (una dirección) distinta y exclusiva para cada uno y para la red que usan, que es en realidad su dirección, al menos mientras están conectados a la red en la sesión correspondiente.

Es importante diferenciar que en el acceso directo y pleno a Internet, el ordenador tendrá la misma dirección siempre, en otro caso, esta dirección puede no ser la misma en cada sesión.

El protocolo ARP, gestiona las direcciones numéricas únicas en Internet, por el que se identifican los ordenadores fisicamente, e inversamente RARP, las determina en sentido contrario.

La dirección IP, unica y exclusiva para cada ordenador, está compuesta de CUATRO NÚMEROS, cada uno de 8 bits en total 4 Bytes =32 bits, con valor entre 0 y 255, separados unos de otros por puntos, que pueden especificar según su orden de izquierda a derecha:

1- El nombre del host, (ordenador)

2- Dominios intermedios: la red, la subred, el nodo, (nombre la empresa) subdominio

3- Por último, el dominio -top level- nacional o internacional de que se trata.

Hay direcciones de distintas clases, que se adaptan al tamaño de cada usuario, dependiendo de la cantidad de redes o anfitriones respectivamente que necesite. Cada clase se identifica, en la dirección IP, por el primero de los cuatro números de que consta la dirección, y dentro de éste, por los primeros bits

Sabemos así que los ordenadores y la información que reciben está identificada e individualizada por el denominado número IP que es consecuencia de la red y del dominio donde se encuentra.

Pero como esta dirección IP es poco amigable y difícil de recordar, para su uso se crearon los NOMBRES DE DOMINIO (DN), que es el equivalente del número IP, pero en palabras mnemónicas. Estas forman grupos separadas por puntos, que indican de la misma forma, el host con un maximo de 63 , dominio y subdominios.

El DNS (Domain Name System) es el sistema de Nombre de Dominio para asignar un nombre a la direccion IP.

La estructura jerarquica del nombre de dominio parte del elemento más singular que es el ordenador para ir abarcando dominios cada vez más grandes, hasta llegar al último que es el país.

Los dominios hay que registrarlos para que cada empresa tenga el uso del dominio en exclusiva, como lo tiene para su denominación, sus marcas o patentes aunque del registro de dominios se encargan organismos no públicos.

Los dominios principales definen el país con dos letras, pero no siempre identifican geograficamente a un pais, ya que se rige por la norma ISO -3166. Algunos ejemplos son:

- Alemania : .de
- Andorra: .ad
- Angola: .ao
- Argentina: .ar
- Armenia: .am
- Australia: .au
- Bahamas: .bs
- Barbados: .bb
- Belgica: .be
- Belize: .bz
- Bolivia: .bo
- Bosnia and Herzegowina: .ba
- Brasil: .br
- Bulgaria: .bg
- Burundi: .bi
- Camerun: .cm
- Canada: .ca
- Colombia: .co
- Corea del Norte: .kp
- Corea del Sur: .kr
- Costa Rica: .cr
- Croacia: hr
- Cuba: .cu
- Chile: .cl
- China: .cn
- Dinamarka: .dk
- Dominica: .dm
- Ecuador: .ec
- Egipto : .eg
- España: .es
- Finlandia: .fi
- Reino Unido: .uk
- Gabon: .ga
- Gambia: .gm
- Gibraltar .gi
- Grecia: .gr
- Guatemala: .gt
- Haiti: .ht
- Holanda: .nl
- Honduras .hn
- India .in
- Indonesia .id
- Iraq: .iq
- Irlanda: .ie
- Islandia: .is
- Israel : .il
- Italia: .it
- Japon: .jp
- Jordania: .jo
- Kenia: .ke

- Kuwait: .kw
- Libia: .ly
- Luxemburgo: .lu
- Madagascar: .mg
- Marruecos: .ma
- Mexico: .mx
- Mongolia: .mn
- Namibia: .na
- Nepal: .np
- Nicaragua: .ni
- Noruega: .no
- Nueva Zelanda: .nz
- Panama: .pa
- Paquistan: .pk
- Paraguay: .py
- Peru: .pe
- Portugal: .pt
- Puerto Rico: .pr
- Suecia: .se
- Tailandia: .th
- Taiwan: .tw
- Tunez: .tn
- Zaire: .zr
- Zambia: .zm
- Zimbabue: zw

EEUU no usa normalmente el suyo (.us)

Los dominios internacionales o genericos de primer nivel son:

- .com: para comercio
- .net: para comercializacion o desarrollo de internet
- .org: para otras organizaciones sin animo de lucro. varios
- .int: Organismo Internacional
- .nato: sede otan
- .gov: agencias del Gobierno
- .mil: ejercito
- .edu: educación. todos los niveles educativos

Los siete nuevos dominios

- .info: proveedores servicio de informacion
- .arts: para entidades dedicadas al arte
- .firm: para negocios y compañias
- .store: tiendas
- .web: actividades relacionadas con la Web
- .rec: para recreo u ocio
- .nom: para webs personales

Los dominios genericos los explotaba la compañía Americana Network Solutions Inc. por acuerdo con el Gobierno EEUU (National Science Foundation), hoy lo hacen tambien otras empresas, ya que termino su gestión monopolisitica en estos registros Internacionales.

8- SOLICITUD DE LOS DOMINIOS

Antes de la solicitud , hay que seleccionar dos o tres nombre de dominio. Después se debe comprobar si ya existe . La consulta se puede hacer on-line, en la base de Datos de Red-Iris o Internic en las direcciones <http://www.nic.es>. Además conviene registrar el dominio como marca y tener preparada una web-site con los DNS,s configurados, en una empresa de servicios de Internet. La solicitud puede hacerse desde Internet.

La solicitud del Dominio de segundo nivel bajo el Top Level Domain (.es) asignado a España , se debe hacer en la actualidad en Red Técnica Española de Televisión, antes Red Iris, dependiente del CSIC (Consejo Superior de Investigaciones Cientificas). En el solo podian registrarse: dominios de organizaciones legalmente estable-

cidas en España y se exige certificado. Es decir personas jurídicas de derecho publico o privado constituidas registralmente, como: Administraciones publicas; Organismos Autónomos; Colegios Profesionales; Cámaras Oficiales; Partidos Políticos; Sindicatos; Asociaciones; Fundaciones; Universidades; Entidades religiosas; Iglesias; sociedades Mercantiles, otras debidamente registradas (escritura constitución). Con un dominio máximo por empresa, y tenia que tener relación directa con el nombre de la empresa o de alguna marca registrada.

Hoy , tras la publicacion de la ORDEN DE 21 DE MARZO DEL 2000, por la que se regula el Sistema de Asignacion de Nombres de Dominio de Internet bajo el Código de País correspondiente a España (.Es). se limina la *restricción en cuanto al número de nombres asignables por organización. Da una razonable protección* para los propietarios de marcas y denominaciones sociales. Posibilita que las personas físicas puedan recibir la asignación de nombres de dominio. Permite la entrada del sector privado en esta actividad, asesorando y tramitando las solicitudes de los usuarios, con arreglo a las normas aplicables.

Los nombres de dominio asignados con anterioridad conservarán su validez, sin perjuicio de que les resulte de aplicación lo dispuesto en ella.

Si la solicitud es de un dominio de primer nivel genérico (.com; .org; .net;..) Se deberá acudir ha alguna de las *empresas delegadas por el ICANN, pues como ya dijimos el monopolio por parte de NSI* ha desaparecido. INTERNIC no restringe el registro y cualquier persona física o jurídica puede solicitar y obtener el dominio sin necesidad de certificado. En principio el principal requisito es que nadie haya inscrito el nombre de dominio antes, aunque se exige bajo criterios de buena fe el uso licito y la tenencia legal del nombre de dominio. Se dice que los dominios caen dentro de la primera enmienda. No obstante se someten a la sentencia y mientras dura el proceso de impugnación queda en suspenso el nombre de dominio.

Para la formación de los nombres de dominio de la empresa se emplean letras (a-z) números (o-9), y guión. Pero hay que tener en cuenta:

- Que el nombre de dominio esta sujeto a una sintaxis y alfabeto concreto el Ingles.

- La longitud del dominio para INTERNIC sera como mínimo dos caracteres y máxima 22 caracteres.

En caso de que no este registrado, es conveniente registrarlo previamente como marca y después como dominio.

Una vez comprobada la posibilidad de usar el nombre, se rellena un formulario On-line indicando:

1- nombre de dominio que se desea y tipo (.com; .es; etc.)

2- Organización usuaria del nombre de dominio: nombre; forma jurídica; NIF; domicilio, calle, municipio, código postal, país.

3- Si el nombre de dominio lo hemos asociado a una marca, indicar él numero de inscripción y la fecha de concesión.

4- Indicar una persona de contacto dentro de la organización solicitante para temas administrativos: nombre y apellidos; nombre de la organización completo; nombre del departamento; cargo; domicilio; dirección de correo electrónico; teléfono; fax; NIF.

Se debe tener en cuenta que una vez que Red Iris conceda el dominio, enviara un formulario, que deberá devolverse firmado precisamente por la persona que indiquemos aquí como contacto para temas administrativos.

5- Persona de contacto para temas de facturación (con red-iris o internic, ...) nombre y apellidos; nombre de la organización completo; nombre del departamento; cargo; domicilio; dirección de correo electrónico; teléfono; fax; NIF.

6- Se indicara también el DNS primario y secundario de nuestro servidor

Las tarifas para uso activo están alrededor de las 12.000, con el mantenimiento del 1er. Periodo (año natural). Mas unas 8000 de mantenimiento anual. IVA incluido.

En Internic se pagan por los dos primeros años 70 dólares y por los siguientes años 35 $.
El tiempo de concesión es más rápido para el registro Internacional (72 horas) que para el nacional que suele estar en dos o tres semanas.

Si lo que queremos es reservar el dominio (inactivo), existen empresas que lo hacen por unas tres mil pesetas año, como rapid Site <http://www.rapidsite.es>; Nominalia ; etc..

Así mismo tendremos que tener contratado el alojamiento de la Web (Hosting) con dominio propio, en alguna empresa comercial.

El Dominio redirigido o gratuito es factible, si el coste o previsión de gasto de un dominio virtual, supera el presupuesto asignado, se puede optar por crear uno redirigido que guiara la petición a otra dirección Web pero con la homepage propio, con lo cual los recursos consumidos se minimizan y el coste desciende significativamente. Hoy también hay empresas (isp) que ceden gratuitamente de 2 a 10 Mb para poder incluir una web aunque el dominio no sea el propio.

El tiempo medio de registro es mayor para el <.es> de unos 20 días y para los genéricos <.com...> 2 días, lo que ha dado lugar a protestas.

Nuestro IPS deberá configurar el servidor introduciendo el DNS primario y secundario para el funcionamiento correcto de la Web, pues aquí es donde se redicionara la petición del numero por el DNS.

9- NUEVA REGULACION DEL DOMINIO ".ES " EN INTERNET, DICTADA POR EL MINISTERIO DE FOMENTO ESPAÑOL.

-La Orden 21-3-2000, regula la asignación de Nombres de Dominio de Internet correspondiente a España (.Es). (B.O.E. 30-3-2.000). Distingue bajo el indicativo de país correspondiente a España (".es") entre nombres de dominio de segundo nivel REGULARES, que podrán ser utilizados por los interesados que tengan derecho a ellos, previa su comprobación, confiriendo el derecho exclusivo de su utilización a efectos de direccionamiento en "Internet" y nombres de dominio ESPECIALES, designados por la Secretaría General de Comunicaciones previa consulta con el Comité Consultivo sobre Nombres de Dominio y limitados a aplicaciones concretas, tales como genéricos y topónimos, con las condiciones que se especifiquen, en cada caso, pero siempre en caso de notable interés social, comercial o de índole nacional, o con el propósito de agilizar la presencia en Internet de los interesados la nombres de dominio especiales, incluidos los genéricos y topónimos, para su utilización, sin sujeción a las normas de los "regulares" a excepción de las normas de sintaxis.

Habilita a la Secretaría General de Comunicaciones podrá dictar las resoluciones necesarias

La Comisión para la Supervisión del Servicio de Acceso a la Información, asumirá las funciones de estudio, deliberación y elaboración de propuestas, recabando información de la Oficina Española de Patentes y Marcas y del Registro Mercantil Central.

La Autoridad de asignación implantara, mantendrá y operara la base de datos necesaria para el funcionamiento del sistema. Asegurando el buen funcionamiento del sistema y la continuidad del servicio, garantizando la calidad del servicio prestado.
Sus decisiones podrán ser recurridas ante la Secretaría General de Comunicaciones.

El ANEXO de esta Ley fija Las NORMAS para la asignación de nombres de dominio regulares bajo el código de país correspondiente a España (".es"), que transcribimos a continuacion por su actualidad:

Disposición general.

Al margen de los requisitos y prohibiciones establecidos en las presentes normas, los nombres de dominio regulares se asignarán al primer solicitante que tenga derecho a ello.

2. LEGITIMACION PARA LA OBTENCION DE UN NOMBRE DE DOMINIO REGULAR.

2.1 Podrán recibir la asignación de un nombre de dominio regular las personas físicas y las organizaciones legalmente constituidas, entendiendo como tales todas las personas jurídicas de derecho público o privado debidamente constituidas.

2.2 No podrán recibir la asignación de nombres de dominio regulares las entidades sin personalidad jurídica, como las sucursales, departamentos, delegaciones, secretarías, consejerías, concejalías o demás partes de una organización, que habrán de ampararse bajo un dominio asignado para toda la organización de la cual dependan, con la excepción prevista en el apartado siguiente.

2.3 No obstante lo previsto en los apartados anteriores, podrán recibir la asignación de un nombre de dominio regular los Departamentos Ministeriales de la Administración General del Estado y las Consejerías de las Comunidades Autónomas.

3. NOMBRES DE DOMINIO REGULARES PERMITIDOS.

3.1 Un nombre de dominio regular podrá ser asignado si reúne los siguientes requisitos:

(a) No estar previamente asignado.

(b) Cumplir las normas de sintaxis (apartado 3.2).

(c) No estar comprendido dentro de las prohibiciones (apartado 3.3).

(d) Cumplir las normas generales de derivación de nombres de dominio (apartado 3.4).

3.2 Normas de sintaxis:

(a) Los únicos caracteres válidos para un nombre de dominio son las letras del alfabeto inglés ("a" - "z"; el sistema de nombres de dominio no distingue entre mayúsculas y minúsculas), los dígitos ("0" – "9") y el guión ("-").

(b) El primero y el último carácter del dominio no puede ser el guión.

(c) La longitud mínima admitida para un dominio de segundo nivel es de 3 caracteres (la mínima recomendada para disminuir la probabilidad de conflictos es de 5 caracteres).

(d) La longitud máxima admitida para un dominio de segundo nivel es de 63 caracteres (la máxima recomendada, por motivos prácticos, es de 24 caracteres).

3.3 Prohibiciones:

En ningún caso se admitirá la asignación de un nombre de dominio regular que:

(a) Coincida con algún nombre de dominio de primer nivel (por ejemplo: "edu", "com", "gov", "mil", "org", "int", "net", "arpa"), o bien con uno de los propuestos por alguno de los grupos u organizaciones de reconocida autoridad en "Internet" (por ejemplo: "firm", "store", "web", "arts", "rec", "info", o "nom").

(b) Se componga exclusivamente de un topónimo (por ejemplo: países, regiones, provincias, comarcas, municipios, pueblos, islas, gentilicios, montañas, mares, lagos, ríos o monumentos).

(c) Se componga exclusivamente de un genérico (o su abreviatura) de productos, servicios, establecimientos, sectores, profesiones, actividades, aficiones, religiones, áreas del saber humano, tecnologías, clases o grupos sociales, enfermedades, especies animales, vegetales o minerales, cualidades o características de las personas, los seres vivos o las cosas.

(d) Coincida con nombres de protocolos, aplicaciones y terminología de "Intenet" (por ejemplo: "telnet", "ftp", "email", "www", "web", "smtp", "http", "tcp", "dns", "wais", "news", "rfc", "ietf", "mbone", o "bbs").

(e) Se componga, exclusivamente, de una combinación de los casos contemplados en los tres apartados anteriores.

(No obstante, podrá admitirse la asignación de nombres de dominio regulares que se compongan, exclusivamente, de una combinación de los casos contemplados en los tres apartados anteriores cuando dicha combinación identifique, de forma inequívoca, a la organización solicitante. Este supuesto, sólo será de aplicación para organismos públicos y organizaciones de indiscutible reconocimiento por el público en todo el Estado.)

(f) Incluya términos o expresiones que resulten contrarios a la Ley, a la moral o al orden público.

(g) Se asocie de forma pública y notoria a otra organización, acrónimo o marca distintos de los del solicitante del dominio.

(h) Se componga, exclusivamente, de nombres propios o apellidos, salvo cuando se corresponda literalmente con una marca o nombre comercial registrado en la Oficina Española de Patentes y Marcas a nombre de la organización solicitante del dominio. Ello se entiende sin perjuicio de la asignación, sin las citadas restricciones, de subdominios a las personas físicas.

(i) Se componga, exclusivamente, de una secuencia de dígitos, salvo cuando se corresponda literalmente con una marca o nombre comercial registrado en la Oficina Española de Patentes y Marcas a nombre de la organización solicitante del dominio.

Las prohibiciones establecidas en los apartados b), c) y e) precedentes, no serán de aplicación a las solicitudes de nombres de dominio que reproduzcan literalmente el de la organización solicitante del dominio, tal como aparezca en el Registro público correspondiente, o el de una de sus marcas o nombres comerciales registrados en la Oficina Española de Patentes y Marcas.

En el caso de las sociedades mercantiles, la denominación social ya incluye su forma social o abreviatura. Para el resto de organizaciones indicadas en la sección 2, el nombre de dominio deberá ser cualificado con la forma social correspondiente.

3.4 Normas generales de derivación de nombres de dominio:

3.4.1 Sólo se podrán asignar como nombres de dominio regulares los siguientes:

a) El nombre completo de la organización, tal y como aparece en su escritura o documento de constitución.

(b) Un acrónimo del nombre completo de la organización lo más cualificado posible, de forma que sea directa y fácilmente asociable al nombre oficial de la organización. Preferentemente un acrónimo habitualmente usado por la organización y legalmente registrado en la Oficina Española de Patentes y Marcas.

(c) Una o varias denominaciones comerciales o marcas legalmente registradas en la Oficina Española de Patentes y Marcas. No se admitirán rótulos de establecimientos, dado su carácter local.
(Las personas físicas sólo podrán recibir la asignación de los nombres de dominio previstos en el apartado (c), esto es, las denominaciones comerciales o marcas registradas de las que sean titulares.)

3.4.2 No se permitirá a ninguna organización recibir la asignación de un acrónimo que no se corresponda razonable e intuitivamente con el nombre oficial de dicha organización.

3.4.3 Tampoco se admitirán dominios que incorporen comodines o coletillas (tipo sufijo "net " o prefijo "inter", etc.) que no tengan relación alguna con el nombre oficial de la organización solicitante.

3.4.4 Cuando de la aplicación de las presentes normas generales de derivación de nombres de dominio resulte uno en contradicción con lo dispuesto en los apartados 3.2 y 3.3, el nombre de dominio no será admitido y habrá de ser modificado o cualificado de tal forma que cumpla dichas normas.

Esto es así incluso cuando el nombre de dominio propuesto se corresponda literalmente con el nombre completo de la organización solicitante o con el de una de sus marcas registradas.

Por ejemplo, si contiene caracteres no permitidos, éstos habrán de ser sustituidos por otros afines (por ejemplo, "ñ" por "n" o "ny"); si el nombre de dominio resulta ser un genérico o toponímico habrá de ser cualificado con la forma jurídica de la organización (por ejemplo, "-sa", "-sl", "-sc", "fundacion-" o "fund-", "asociacion-" o "asoc-") o, si se tratara de una marca, con el número de entre las 42 clases del nomenclátor internacional de productos y servicios bajo la que está registrado por la organización solicitante del dominio (por ejemplo, "-38", "-c38" o "-clase 38").

4. TERMINOS Y CONDICIONES DE ASIGNACION DE NOMBRES DE DOMINIOREGULARES

4.1 La responsabilidad última del uso de un nombre de dominio regular recae siempre sobre la organización para la que se haya registrado dicho dominio. En concreto, un proveedor de servicio "Internet" no es responsable administrativo de un dominio asignado a una organización a la que dé servicio; esto es así independientemente de que el proveedor haya hecho de intermediario para la asignación de dicho dominio o de que el proveedor esté gestionando, por delegación de la organización, el servidor primario para la zona de segundo nivel asociada al mencionado dominio.
Una organización puede conservar el mismo nombre de dominio regular independientemente de cambios de proveedor o de que esté conectado a varios proveedores simultáneamente.

4.2 En toda petición de asignación de nombres de dominio regulares, la persona designada como intermediario para cuestiones administrativas deberá contar con poder suficiente de representación de la organización para la cual se solicita.

4.3 La asignación de nombres de dominio regulares sólo tendrá validez mientras se mantengan las condiciones que dieron lugar a aquélla.La asignación de los nombres de dominio regulares perderá efecto cuando se compruebe la existencia de la nulidad de la inscripción o se acredite por la Administración la pérdida del derecho al mantenimiento de la titularidad del nombre por su titular.

4.4 Los beneficiarios de la asignación de nombres de dominio regulares, deberán informar inmediatamente a su agente de todas las modificaciones que se produzcan en los datos asociados con ella.

4.5 La asignación de un nombre de dominio regular no confiere ningún derecho sobre el mismo, salvo el de su utilización a efectos de direccionamiento en el sistema de nombres de dominio de "Internet".

4.6 La autoridad de asignación no será, en ningún caso, responsable por la vulneración de derechos de propiedad intelectual o industrial, o de cualesquiera otros derechos o intereses legítimos que puedan derivarse de ella.

Tampoco serán, en ningún caso, responsables por las posibles vulneraciones a que se refiere el párrafo anterior, el personal y los representantes de la autoridad de asignación.

La otra norma que completa el nuevo marco legislativo es la RESOLUCIÓN DE 10 DE FEBRERO DE 2000, de la Secretaría General de Comunicaciones-En virtud de lo previsto en el artículo 27.13 del Reglamento por el que se desarrolla el Título II de la Ley General de Telecomunicaciones , aprobado por Real Decreto 1651/1998, de 24 de julio-, DESIGNA PARA LA GESTIÓN DEL SISTEMA DE NOMBRES DE DOMINIO (.ES):AL ENTE PUBLICO RED TÉCNICA ESPAÑOLA DE TELEVISIÓN como autoridad competente para la gestión del registro de los nombres de dominio de internet bajo el código de país correspondiente a españa. Este cometido era desempeñado hasta ahora por el Consejo Superior de Investigaciones Científicas, que aunque habia recibido algunas criticas por alguna norma de inscripcion, lo gestiono de una manera eficaz en consonancia con sus medios, impidiendo que se extendiese la actividad especulativa de los ciberokupas en".es" y permitiendo ahora aprovechar su experiencia acumulada.

La nueva regulacion permitira alosabogados registrarsebajo ".es " . Ademas el nombre de dominio se coordinara con el Registro Mercantil Central, la Oficina Española de Patentes y Marcas y demás Registros Públicos Nacionales e Internacionales.

El objeto es evitar los conflictos que genera el uso indebido o ilicito del nombre de dominio en relacion con las marcas y demas registros.

Sabido es que el sistema de nombres de dominio (DNS), desarrollado por el ya fallecido Dr. Jonathan B. Postel director de la IANA, se emplea en "Internet" para identificar unívocamente a los equipos conectados a la red, a traves de nombres en lugar de números que son más difíciles de memorizar.

Su estructura apoyada en una gran base de datos distribuida jerárquicamente en muchos servidores por toda la red, permite, entre otras a una organización mantener e independizar sus equipos en función de aspectos cambiantes, tales como la topología de la red y el proveedor de acceso a "Internet" y aliviar la carga de gestión del administrador central, entre los distintos subadministradores de los distintos niveles de dominios delegados.

En el nivel más alto de la jerarquía de "Internet" se encuentran los dominios de primer nivel, territoriales de dos letras según código ISO-3166 , en el caso de España es: ".es". al que se refieren las normas recién publicadas que comentamos.

Los dominios internacionales genéricos (gTLDs) de tres letras (como ".com", ".net" u ".org"), están controlados y regulados por el ICANN (Internet Corporación for Assigned Names and Numbers) http://www.icann.org Corporación de Internet para la Asignación de Nombres y Números (Nonprofit Public Benefit Corporation) que sustituyo a la IANA y que cuenta entre sus áreas una especifica de Dominios -DNSO (Domain Name Supporting Organization).

ES-NIC RESPONDE DE LA GESTIÓN DEL DOMINIO DE DNS DE PRIMER NIVEL PARA ESPAÑA (".ES"), como "Registro Delegado de Internet en España", dentro del servicio a la comunidad Internet de los NICs (Network Information Centers).

Entre sus funciones esta la de Registro de nombres de dominio. Pero las direcciones IP se obtienen a través del proveedor que facilite el acceso a Internet.

REFERENCIAS :

- froomkin, a. michael: Anonymity and its Enmities, J. Online L. art. 4 par. Tempoorary homepage located at: < http://acr.law.miami.edu>
- Es-nic: < http://www.nic.es>
- Internic: < http://www.internic.com>
- Internic registro < http://www.rs.internic.net/rs-internic.html>
- El CORE, (Council of Registrars) <http://www.corenic.org>
- Nic: <http://www.nic.es/whois/>
- Faq sobre registro de dominio nic en http://www.rs.internic.net/domain-info/registration-FAQ.html>
- Lista de autoridades de dominio : < http://www.rs.internic.net/help/other-reg.html>
- Corporación de Internet para la Asignación de Nombres <http://www.icann.org>
- Rapid Site <http://www.rapidsite.es
- El "Libro Blanco" elaborado por el Departamento de Comercio norteamericano se puede obtener en: http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm
- Other References:
[1] Cooper, A., and J. Postel, "The US Domain", RFC 1480, USC/Information Sciences Institute, June 1993.
[2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1340, USC/Information Sciences Institute, July 1992.
[3] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, USC/Information Sciences Institute, November 1987.

* Carlos Barriuso Ruiz "La seguridad jurídica en el comercio electrónico" "DNS, NOMBRES DE DOMINIO Y EL COMERCIO ELECTRONICO" ICADE- ESCUELA DE PRACTICA JURIDICA, Universidad Comillas- Madrid ; noviembre 1999

Pornografía, Racismo e Internet

Ezequiel M. Zabale* y Guillermo Beltramone (Argentina)**

I-. INTRODUCCION.

Internet es una red mundial de computadoras nacida y esparcida prácticamente de la nada, en menos de 10 años, la red se ha esparcido en forma contundente llegando a todos los sectores y a todos los países.

Internet no es mágica, no funciona sola, esta compuesta por maquinas pero habitada por hombres, la red es esencialmente humana, su historia y su evolución hacen a la necesidad de comunicarse, de estar en contacto, de transmitir, de dar y recibir.

Por ello la red es solo un reflejo de las personas que la hacen, es un espejo de la sociedad que la forma, que en mas o en menos tiende a generalizarse.

Esto implica que sobre la misma se vuelcan todos los contenidos de la sociedad o más bien de los grupos sociales que la forman, se vuelca el amor, el sentimiento de ayuda, el interés general y así podríamos seguir. Pero a la vez también se vuelca la parte oscura de nosotros mismos que somos quienes formamos la red, por ello también existe venta de armas y drogas, pornografía, paginas donde se enseña a pillar, robar, crackear, y así también podríamos continuar con nuestra enumeración.

II-. PORNOGRAFIA Y RACISMO.

¿Que debemos entender por pornografía?. La pregunta no puede ser menos que vital si queremos comprender el fenómeno delictivo pornográfico en la red.

El diccionario define a la pornografía como el carácter obsceno de una obra del genero artístico en cualquiera de sus expresiones. Esta definición nos lleva a considerar que debe entenderse por obsceno y he aquí el problema, pues la obscenidad es una cuestión personal que tiene que ver con la carga educacional cultural que cada uno de los individuos de un grupo social determinado posea. Por lo que resulta que lo obsceno y pornográfico para uno no lo será para los otros.

En cuanto al racismo puede simplemente definirse como una manifestación de odio o adveración hacia un grupo determinado bien por sus creencias religiosas, por su orientación sexual, por su color o contextura. A diferencia de la pornografía que se ha convertido en placer de masas en el último cuarto del siglo pasado, el racismo acompaña públicamente al hombre –para su deshonor- desde hace unos 2000 años.

III-. DIVERSOS TIPOS DE PORNOGRAFIA Y DIFERENTES FORMAS DE RACISMO.

Existen ciertos parámetros que son tenidos en cuenta para establecer categorías o tipos pornográficos.

* Analista de Sistemas y Abogado. Profesor titular de la Cátedra Taller de Informática Jurídica I y II de la Facultad de Derecho de la Universidad Abierta Interamericana (Sede Regional Rosario). Jefe de Trabajos Prácticos en la Cátedra de Derecho Civil II de la Facultad de Derecho de la Universidad Nacional de Rosario.

** Abogado. Profesor adjunto de la Cátedra Taller de informática I y II de la Facultad de Derecho de la Universidad Abierta Interamericana (Sede Regional Rosario). Profesor Adscripto en la Cátedra del Ciclo de Orientación Definida en Informática Jurídica y Derecho Informático de la Facultad de Derecho de la Universidad Nacional de Rosario.

Los que nos interesan en este caso son dos parámetros, el primero el que distingue entre pornografía legal e ilegal. Esta es una construcción de tipo jurídico, generalmente a través de normas emanadas de los órganos de control[1].

Nos detendremos ahora en la distinción más cruda quizás, que diferencia entre adultos y menores, a esta ultima se la conoce genéricamente con el nombre de "Pornografía Infantil[2]".

En cuanto al racismo, mas haya del legal[3], abarca a todas las formas de discriminación, hacer una clasificación sobre las mismas es algo que excede el ámbito de la presente.

IV-. PORNOGRAFIA Y RACISMO EN LA RED.

No existe ningún estudio serio que haya medido la cantidad de material pornográfico e intolerante que circula por internet pero se estima[4] que alrededor de un 15% de todo el material que circula en la red tienen un contenido erótico, pornográfico y/o intolerante.

Cada servicio de Internet es usado en forma diferente y con propósitos diferentes.

El servicio de Web es uno de los mas requeridos por quienes intentan colocar material de contenido sexual explícito o similar. Se coloca el material en paginas de alojamiento gratuito por un tiempo y luego se mudan[5] y así en forma sucesiva, puede tratarse de fotos, videos, relatos y todo ellos reales o ficticios. En muchas paginas se debe pagar una cantidad ínfima para poder entrar, en otras es totalmente gratis (la mayoría).

Algunos de los autores de las paginas se toman el trabajo de crear un código de verificación de edad a través del cual se verifica que la persona que esta navegando sea mayor de 18[6] años. Los sistemas de verificación[7] de edad requieren el uso de tarjetas de crédito y como no hay demasiadas personas dispuestas a otorgar su numero de tarjeta por la red en general tienden al fracaso lo que lleva al fracaso a la pagina que posee el portal de verificación.

El servicio de e-mail se ha visto afectado en forma indirecta, muchas personas que se dedican a cambiar material explícito (en cualquier formato digital) abren cuentas de webmail en los servicios gratuitos, a veces dos o más para evitar ser localizados lo que lleva a estos sistemas a un virtual estado de paralización en la transferencia de la información. La ventaja del servicio de mail respecto de web esta radicada en la absoluta reserva del contenido de la información, *aquí no hay poder de policía valido por parte del proveedor del webmail*[8].

Por último el IRC[9] es el servicio preferido para intercambiar material de contenido sexual y sobre actos

---

1 Es decir los Institutos de Cine, los Normalizadores, etc.

2 Kiddieporn en ingles.

3 Régimen de Apartheid que sostuvo su efectividad hasta principios de la década del 90 del siglo pasado, los sistemas de casta en algunos lugares de la India y Nepal, etc.

4 Véase por sobre todo www.free.com donde se encuentra interesante material sobre la composición y estructura de la red en todos sus servicios y usos.

5 Los proveedor de alojamiento suelen reservarse facultades de poder de policía, cuando encuentran una pagina que no es del agrado simplemente la eliminan.

6 Que es la edad que la gran masa de legislaciones mundiales fijan para establecer la plena capacidad civil

7 El sistema de verificación mas difundido en Adult Check. Puede verse en www.adultcheck.com. El sistema requiere que se ingrese un numero de tarjeta de crédito valido internacional y se verifican los datos con la central emisora de la tarjeta. Presenta varias deficiencias, entre ellas cabe enumerar la deficiencia en el tratamiento de la información, la perdida de claves y la facilidad de imitación de las claves, a tal punto que existen sitios de Internet donde se ofrecen códigos de Adult Check vigentes y validos que pueden servir para entrar a las paginas protegidas, entre otras puede verse www.islatortuga.com

8 Aunque algunos servidores de Webmail dan de baja las cuentas de sus usuarios al advertir nombres extraños en los ficheros adjuntos.

9 Internet Relay Chat es un servicio de charla en línea, en la jerga chat, los dos programas que dominan el mercado de IRC son el mIRC y el Pirch ambos de muy buena factura técnica.

de discriminación, es anónimo, es rápido y es prácticamente imposible ser rastreado, en un par de horas un sujeto medianamente familiarizado con el uso de computadoras (ya no de Internet sino de computadoras) puede conseguir toda una tienda pornográfica o convertirse en el futuro Hitler. Este es el servicio por excelencia, aquí no hay control, ningún control.

El servicio de IRC presenta además una particularidad, es el lugar por excelencia donde se reúnen pedófilos y pederastas a intercambiar experiencias, fotos, videos y demás a diferencias de los fascistas que prefieren el servicio de Web porque presentar mayor difusión[10].

A diferencia de los restantes servicios donde esta temática es un poco difícil de tratar por la posibilidad de un rastreo[11], en el IRC no hay obstáculos.

Todos los servidores de IRC del mundo tienen sus canales pornográficos, ya sea para hablar sexo, para cambiar material, para hacer encuentros, e incluso sus canales de pornografía infantil. Sin duda en los servidores de Undernet[12] es donde más canales de este tipo existen.

V-. DEBEN SER CONSIDERADO DELITOS LA PORNOGRAFIA Y EL RACISMO EN INTERNET.

La respuesta es más compleja que la pregunta y requiere varios niveles de análisis.

Ante todo debemos ponernos de acuerdo respecto de que ley aplicaremos para determinar si el material es o no pornográfico, presenta o no contenido discriminativo, la ley del lugar de asiento físico del servidor, la ley del lugar donde las paginas se pueden accesar, la ley del lugar físico desde donde se intercambia el material. En cualquier caso este tipo de control es técnica, humana y jurídicamente imposible.

A un segundo nivel, determinada la ley aplicable, a quien debe sancionarse, a los que arman la pagina con contenido sexual, a los que la accesan, a quien provee el alojamiento o prestan su servidor de IRC para intercambiar material. Ello es también muy difícil de decidir e imposible de controlar.

En tercer lugar que sanción deben recibir?!. Dependerá en todos los casos de la suerte de los debates anteriores, pero como imponer la sanción, como dar el ejemplo de la pena, ¿cómo hacer para que la pena cumpla su finalidad ejemplificadora?

Todas estas preguntas quedan en el aire sin una respuesta jurídicamente unívoca que conforme a todos los sectores y que permita una rápida solución el problema planteado.

Pero algo si es indudable, la pornografía infantil, el abuso sexual y los fanatismos debe combatirse en todos los ámbitos, no se trata ya de personas que quieren fotos, se trata de personas que quieren, buscan o cambian videos de otras personas abusando de menores o bien de menores sufriendo vejaciones, o de fanáticos atacando a civiles inocentes, se trata de verdaderas bestias cambiando material harto perverso, se trata de la naturaleza mas vergonzosa del hombre.

[10] Debido a que el IRC es en general de persona a persona, mientras que la Web es una pantalla donde reflejar actos hacia muchos observadores y con menor trabajo.

[11] Por citar un ejemplo, en un proveedor de alojamiento gratuito argentino se había instalado una pagina con contenidos para pedófilos, el hecho fue denunciado entre otros por el diario Clarín y la pagina fue inmediatamente dada de baja. Véase www.clarin.com.ar

[12] Undernet esta compuesta por una serie importante de servidores de IRC ubicados en Europa, principalmente en Holanda y en EE.UU. Como su nombre lo expresa se trata de la red "baja", de la "profunda", de lo que no "se puede ver". Existen algunos canales cuyos nombres ya son bastan de ejemplo, por solo mencionar uno "100%%preteengirlsexpics".

115842

UNIVERSIDAD
BIBLIOTECA
DE LIMA

VI-. PERMITIR O PROHIBIR.

Hemos expuesto en los párrafos anteriores lo difícil que puede ser un control técnico, humano o jurídico sobre este tipo de material circulante.

La pornografía es parte de la vida del hombre y por ello no debemos no debe causar asombro que en este nuevo medio exista material de contenido sexual explícito.

La cuestión entonces es ¿deben permitirse todas las manifestaciones de contenido sexual y/ fanatismos en Internet?, simplemente porque la misma sea un nuevo medio de comunicación y que sus actores sean muy difíciles de ubicar por razones técnicas o humanas, la respuesta indudable –según nuestro punto de vista- es que NO.

Entre otras cosas debemos poner todos los medios para evitar la difusión de material pornográfico infantil, material sobre abuso sexual y de contenidos similar, ya porque pueda afectar a quien lo reciba e incentivarlo a cometer actos similares, ya porque es una doble defraudación a la persona que sufre la vejación[13].

Podemos a esta altura llegar a ciertas conclusiones, 1) debemos combatir la circulación de cierto tipo de material sexual en la red y fuera de la misma aun sin haber llegado a un acuerdo sobre la legislación aplicable pues tal tipo de material es inaceptable 2) La lucha es dificultosa por las barreras físicas, técnicas y humanas que dificultan la tarea, pero ello no debe implicar un abandono de la cosa.

VII-. LO QUE TENEMOS NO ALCANZA.

Cuando se ha intentado combatir al crimen organizado la lucha tuvo que ser organizada, así surgió la Interpol, el intercambio de información y la legislación internacional sobre crimen financiero, etc.

Hay intentos aislados de combatir las manifestaciones no deseadas, un caso paradigmatico es el de Marc Dutroux conocido pedófilo belga que fuera capturado por la policía, sentenciado e increíblemente se escapo de sus guardias, entre sus pertenencias se habían encontrado gran numero de vídeo infantiles, fotos y un disco rígido completo de pornografía infantil[14].

Otro caso critico que refleja las dificultades que tienen la autoridades de comprender el uso de la nueva tecnología ha sido el caso Felix Somm, mas conocido como caso Compuserve. La empresa de capitales alemanes y americanos brindaba desde sus servidores en Alemania acceso mundial a BBS con contenidos pedófilos y juegos altamente violentos como DOOM y Heretic. Procedida la denuncia en EE.UU se allanaron las sedes de la empresa en Alemania y Felix Somm fue encontrado penalmente responsable de contribuir al delito de divulgación de pornografía infantil[15].

Otros intentos vanos han sido por ejemplo los del gobierno australiano que ha creado un organismo oficial el Australian Broadcasting Authority (ABA), que deberá regular el contenido de Internet según una ley sancionada por la legislatura australiana.[16] A mas de tres meses de su entrada en vigencia aun no e ha procedido a marcar o censurar material alguno.

Podemos seguir citando ejemplos de lucha asilada y desorganización, donde se confunden conceptos básicos, se pena al PAI y no al pornógrafo, se trata de censurar los efectos pero no se combaten las causas.

---

13 No solo es abusada sexualmente, sino que además deberá soportar que su imagen sea transmitida por Internet en forma indefinida.

14 Puede verse la crónica en El Universo Digital, Caracas, viernes 24 de abril, 1998.

15 Puede verse mas material sobre el caso en derecho.org ediciones de octubre de 1998.

16 Véase www.aba.gov.au o bien el suplemento informática de Clarin en www.clarin.com.ar del 29/12/1999

VIII-. MEDIDAS POSIBLES PARA COMBATIR LA PORNOGRAFIA INFANTIL Y EL RACISMO EN INTERNET.

Preliminarmente, debemos reiterar que no es la intención nuestra comenzar una caza de brujas en Internet, ni pretendemos purificar a la red, ni nada por el estilo, solo procuramos evitar la difusión de material altamente ofensivo.

Que medidas podemos proponer desde este lugar a fin de lograr una combinación de fuerzas que permitan la formación de un frente de lucha contra este tipo de manifestaciones u otras similares[17].

1. Los proveedores de alojamiento, ya sea gratuito o de pago, deben intensificar su poder de policía y registrar con mayor asiduidad el contenido de las paginas que aloja su host. No se trata de dar poder en forma indiscriminada al proveedor porque esto podría llevar a la situación contraria a la deseada, se trata de lograr que los proveedores de alojamiento hagan a un lado su política de ventas y observen que cosas están alojando. Es sabido que las paginas que más ingresos de personas reflejan son las de contenido sexual y por ello mas publicitan. Si logramos convencer al proveedor de alojamiento y al publicista que los sitios que contienen material sobre abuso de menores o similar no son un buen sitio para dar a conocer un producto tendremos un aliado fundamental en la lucha que pretendemos encarar.

2. Crear una división dentro de alguno de los muchos organismos internacionales[18] de lucha contra el crimen organizado a fin de usar Internet como medio para combatir los crímenes de abuso sexual contra menores o adultos y las manifestaciones de racismo, usando la misma red pero para beneficio. Por ejemplo, usar el servicio de IRC, entrar a los canales de pornografía infantil, tratar de obtener datos sobre las personas que intercambian[19], trabajar en coordinación con el OP del servidor a fin de lograr identificar desde donde acceden cada uno de los users del canal. A la vez intercambiar material a fin de lograr identificar a las víctimas y a los victimarios[20]

3. Trabajar en conjunto con las organizaciones que buscan chicos desaparecidos, las que trabajan con chicos abusados sexualmente y las que buscan combatir las manifestaciones de violencia racial en cualquiera de sus formas a fin de intercambiar material, cruzar notas y establecer vínculos y relaciones.

4. Procurar normativa legal supraestatal para combatir la distribución de material sobre abuso de menores y/o sexual en cualquier especie, la difusión de material sobre violencia racial en cualquiera de sus formas y variantes.

5. Educar a padres, maestros y alumnos sobre el uso consciente de la red, sobre un uso adecuado para la Internet.

6. En definitiva lograr unificar esfuerzos dentro y fuera de la red a fin de combatir las manifestaciones antes indicadas, tanto en la medida que sucedan como en la medida que sean distribuidas por Internet, aprovechando las ventajas que nos ofrece la red y cargándolas en perjuicio de quienes intentamos identificar.

IX-. CONCLUSIONES.

Como corolario de lo expuesto podemos decir extraer las siguientes conclusiones, a saber:

- Internet es una nueva forma de difusión de contenidos de todo tipo.

---

[17] Tal el caso de material sobre racismo, discriminación contra minorías étnicas, sexuales o religiosas.
[18] ONU, OEA, Interpol, etc.
[19] A través de scripts, ingeniería social, etc.
[20] Siempre que aparezca una caro o rostro visible puede saberse el origen étnico, la zona geográfica de donde son oriundos víctima y victimario, comunicarse con las autoridades locales, establecer busquedas, es decir alguien debe conocer a estas personas, escuelas, instituciones intermedias, etc.

- No debemos tolerar la difusión de material sobre aberraciones sexuales o crímenes raciales, sin que ello implique crear una nueva caza de brujas.

- Los intentos actuales por combatir este tipo de crímenes han sido verdaderos fiascos, han triado mas confusión que mejorías a la situación en general debido a la falta de calificación de los actores del proceso judicial respecto de estos temas, confundiendo así conceptos básicos y creando aun más caos.
- Adoptar una o varias de las medidas propuestas en el presente trabajo a fin de lograr un combate efectivo y dinámico contra las manifestaciones descriptas.

- Concensuar nuevas formas de control sobre el material en circulación siempre salvaguardando la libertad del individuo.

El Derecho Telemático: Respuesta a la Convergencia Tecnologica*

Dr. Carlos E. Delpiazzo** (Uruguay)

I) INTRODUCCION

A partir de la convergencia de la Informática y las Telecomunicaciones (1) y en función de las importantes transformaciones experimentadas en el campo de estas últimas (2), entre otras razones como consecuencia de su potenciación por la primera, hoy es posible hablar de un naciente Derecho Telemático.

El uso de la expresión "telemática" fue inicialmente propuesto por los autores del informe presentado en 1978 al entonces Presidente de Francia, Valery Giscard d' Estaing, y publicado ese mismo año bajo el título de "La informatización de la sociedad" (3), para designar la imbricación creciente de los computadores y de las telecomunicaciones.

El nuevo símbolo lingüístico tuvo rápida fortuna, siendo ampliamente difundido a partir de 1980 (4) y abriendo camino hacia la construcción de un novedoso modelo de sociedad signado por lo que se ha dado en llamar la "utopía telemática" (5).

Hoy, el horizonte telecomunicativo resulta inconmensurablemente expandido por las "autopistas de la información" que surcan el planeta constituyendo una verdadera red de redes en la que la televisión, la telefonía y los computadores convergen para trasmitir sonido, imagen, datos y textos a través de líneas telefónicas, fibras ópticas, cables submarinos y enlaces satelitales. Esta realidad augural de un mundo diferente (6) no es sólo un producto tecnológico sino que involucra connotaciones políticas (7), económicas, sociales y culturales (8) con significativas proyecciones en el campo jurídico (9).

(*) Ponencia preparada para el Tema 1, "Derecho e Internet en el nuevo milenio", del VII Congreso Iberoamericano de Derecho e Informática (Lima, 24 al 29 de abril del 2000).

(**) Doctor en Derecho y Ciencias Sociales por la Universidad Mayor de la República Oriental del Uruguay. Profesor de Derecho Público, Profesor de Informática Jurídica, y Director del Instituto de Derecho Informático en la Facultad de Derecho de dicha Universidad. Profesor de Derecho Administrativo, Director del Programa Master de Derecho Administrativo Económico (PMDAE), y Profesor de Derecho Informático en la Facultad de Derecho de la Universidad de Montevideo. Profesor de Informática Jurídica en la Facultad de Derecho de la Universidad Católica del Uruguay. Presidente del Comité Organizador del VI Congreso Iberoamericano de Derecho e Informática (realizado en Montevideo del 4 al 8 de mayo de 1998). Asesor Letrado de la Cámara Uruguaya de Software.

(1) Carlos E. DELPIAZZO - "Información, Informática y Derecho" (A.M.F., Montevideo, 1989), pág. 95 y sigtes.

(2) Carlos E. DELPIAZZO - "Transformaciones del régimen jurídico de las telecomunicaciones", en VIII International Congress on Computer and Telecommunication Law (San Pablo, 1994), cap. 11; y en Rev. Uruguaya de Derecho Constitucional y Político (Montevideo, 1996), tomo XII, pág. 116 y sigtes.

(3) Simón NORA y Alain MINC - "La informatización de la sociedad" (F.C.E., México, 1980), pág. 29 y sigtes.

(4) Jean Jacques SERVAN SCHREIBER - "Desafío Mundial" (Plaza & Janes, Barcelona, 1982), especialmente pág. 243 y sigtes.

(5) Vittorio FROSINI - "Informática y Derecho" (Temis, Bogotá, 1988), pág. 129 y sigtes.

(6) Bill GATES - "Camino al Futuro" McGraw-Hill, Madrid, 1995), especialmente pág. 65 y sigtes.

(7) Ver: Informe BANGEMANN - "Europa y la sociedad de la información planetaria" (Recomendaciones al Consejo Europeo, 1994, según traducción publicada en DAT, Año VII, Nº 84-85, pág. 20 y sigtes.; e Informe LEHMAN - "Intellectual Property and the National Information Infrastructure" (Washington, 1995), especialmente pág. 177 y sigtes.

(8) Emilio SUÑE LLINAS - "El teletrabajo", en Rev. Iberoamericana de Derecho Informático (U.N.E.D., Mérida, 1998), Nº 19-22, pág. 585 y sigtes.

(9) Antonio MILLE - "La problemática jurídica de las autopistas de la información en los trabajos hemisféricos y en los documentos oficiales estadounidense y europeo", en Rev. Derecho de la Alta Tecnología (Buenos Aires, 1995), Año VII, Nº 84-85, pág. 1 y sigtes.

Así, puede decirse que el Derecho Telemático es el nuevo nombre del Derecho de las Telecomunicaciones, entendidas éstas en su más amplio sentido como comunicaciones a distancia ya no sólo telegráficas, telefónicas y radioeléctricas sino a través de cualquier medio idóneo para el diálogo entre sujetos situados en distintos paralelos y meridianos.

II) CARACTERIZACION DEL DERECHO EMERGENTE

A partir de la caracterización descriptiva precedentemente formulada, es posible esbozar los principales rasgos que perfilan este nuevo Derecho emergente.

En primer lugar, es fácil constatar que el origen y el desarrollo del Derecho Telemático se encuentran asociados a la espectacular evolución de las telecomunicaciones en los últimos años, singularizada por la globalización, el cambio tecnológico y la reestructuración de los servicios (10).

En segundo lugar, el Derecho Telemático está determinado por el dinamismo de las telecomunicaciones como sector de la economía, el cual se encuentra hoy en un proceso de transición desde el monopolio hacia la competencia en materia prestacional (11). En efecto, hasta comienzos de los años ochenta, en general existía en cada país un único operador, titular para su demarcación territorial de un derecho exclusivo para la provisión de redes y servicios de telecomunicaciones organizado en base a dos modelos fundamentales (12), a saber:

a) el llamado modelo de los P.T.T. ("Post, Telegraph and Telephone"), en virtud del cual la regulación, gestión y financiación de las telecomunicaciones, consideradas como un servicio de titularidad estatal, se encomiendan a un organismo estatal; y

b) el modelo de los Estados Unidos, donde las telecomunicaciones no se consideran como un servicio a cargo del Estado sino como una actividad librada a la iniciativa privada, aunque fuertemente regulada y controlada por aquél.

En tercer lugar, como lógica consecuencia de lo que viene de decirse, el Derecho Telemático "combina el ánimo liberalizador con el mínimo común denominador de una regulación necesaria e imprescindible" (13). Tal liberalización obedece a tres causas fundamentales:

a) tecnológicas, ya que la digitalización de la información conduce a la multifuncionalidad de los operadores, de modo que ya no es necesario tener diversos tipos de información con códigos distintos que dan lugar a terminales y redes de transmisión diferentes puesto que hoy se transmite por cualquier tipo de red todo tipo de información;

b) económicas, ya que las telecomunicaciones, que en los años sesenta eran consideradas el tejido nervioso de las sociedades avanzadas, a partir de los ochenta constituyen su sistema circulatorio y son consideradas el motor de las economías modernas; y

c) políticas, ya que el desvanecimiento de las fronteras nacionales para las comunicaciones a distancia y la reconducción del concepto de servicio público han aparejado un nuevo enfoque del sector.

---

(10) U.I.T. - "Informe sobre el Desarrollo Mundial de las Telecomunicaciones" (Ginebra, 1994), pág. 11 y sigtes.

(11) Adolfo CASTILLA - "Economía y regulación en las telecomunicaciones", en Derecho de las Telecomunicaciones (La Ley-Actualidad S.A., Madrid, 1997), pág. 869 y sigtes.

(12) Javier CREMADES GARCIA - "El Derecho de las Telecomunicaciones en Europa y España", en Derecho de las Telecomunicaciones cit., pág. 9 y sigtes.

(13) José Francisco ESTEVEZ RODRIGUEZ - "El Derecho europeo de las telecomunicaciones", en Derecho de las Telecomunicaciones cit., pág. 182 y sigtes.

En cuarto lugar, contrariamente a lo que podría inducir a pensar el señalado proceso de liberalización, la disciplina de la telemática debe reputarse propia del Derecho público (14) y con una fuerte presencia del Derecho internacional en su desenvolvimiento (15).

En quinto lugar, fácil resulta inferir de los caracteres precedentemente enumerados, que el Derecho telemático es por demás novedoso y sumamente técnico, aún en sus aspectos regulatorios, tanto a nivel interno de cada Estado como en el ámbito regional e internacional.

Finalmente, partiendo de la multiplicidad de significaciones que convoca la expresión "autonomía" (16), parece indiscutible proclamar la conveniencia de la autonomía didáctica del Derecho Telemático, sin que ello implique desconocer la autonomía que deriva de la consideración técnica unitaria de su expansivo objeto.

III) IMPACTO DE LA CONVERGENCIA EN LO PRESTACIONAL

Durante muchos años se ha considerado en forma pacífica que las telecomunicaciones constituyen un servicio público. Sin embargo, la realidad actual del explosivo desarrollo telemático ha "hecho saltar por los aires" los cómodos esquemas con que han venido encuadrándose las telecomunicaciones tradicionales (17).

Es que la propia noción de servicio público -quizás una de las más arduas que se pueda enfrentar en el ámbito del Derecho administrativo (18)- se encuentra hoy requerida de una reconstrucción histórica y conceptual (19).

A comienzos de siglo, necesidades prácticas y no meras especulaciones teóricas fueron las que llevaron a la doctrina francesa a intentar superar la ausencia de textos claros que deslindaran la competencia de los tribunales administrativos frente a los tribunales judiciales comunes mediante un principio general que permitiera reconocer cuáles son los litigios de competencia del juez administrativo, trazando las fronteras con la jurisdicción judicial. En ese contexto, los autores de la escuela de Burdeos establecieron como criterio definidor del Derecho administrativo y, por ende, de la jurisdicción administrativa, el del servicio público (20), caracterizado esquemáticamente por tres elementos básicos:

a) un elemento teleológico, significado porque se tratara de una actividad tendiente a satisfacer necesidades de interés general;

b) un elemento subjetivo u orgánico, consistente en que la actividad estuviera a cargo de una entidad estatal; y

c) un elemento formal, expresado en que la actividad se regule primordialmente por el Derecho público.

La amplitud de tal noción encerró el germen de su crisis, conduciendo a su posterior acotamiento para designar el conjunto de actividades desarrolladas por entidades estatales o por su mandato expreso, para satisfacer necesidades colectivas impostergables mediante prestaciones suministradas directa e inmediatamente a los individuos, bajo un régimen de Derecho público (21).

---

(14) Tomás DE LA QUADRA SALCEDO - "Telecomunicaciones y Derecho público", en Derecho de las Telecomunicaciones cit., pág. 131 y sigtes.
(15) Jean Michel ARRIGHI y Roberto PUCEIRO RIPOLL - "Régimen internacional de las telecomunicaciones", en Derecho Internacional Público (Obra dirigida por Eduardo JIMENEZ DE ARECHAGA, F.C.U., Montevideo, 1996), tomo III, pág. 385 y sigtes.
(16) Carlos E. DELPIAZZO, Alvaro J. EIRIN y Pedro J. MONTANO - "Introducción a la Informática Jurídica y al Derecho Informático" (A.M.F., Montevideo, 1984), pág. 132 y sigtes.
(17) Eduardo GARCIA DE ENTERRIA - "Prólogo" a Derecho de las Telecomunicaciones cit., pág. 5 y sigtes.
(18) Rubén Miguel CITARA - "El servicio público" (E.C.A., Buenos Aires, 1995), Parte I, pág. 21.
(19) Jorge Luis SALOMONI - "Teoría general de los servicios públicos" (Ad-Hoc, Buenos Aires, 1999), pág. 17.
(20) Ver: Jorge SILVA CENCIO - "Servicio público y concesión de servicios" (A.M.F., Montevideo, 1980), pág. 15 y sigtes.
(21) Así: Enrique SAYAGUES LASO - "Tratado de Derecho Administrativo" (Montevideo, 1959), tomo I, pág. 65.

De tal definición ajustada se desprende la vinculación de la noción de servicio público con la de exclusividad (o monopolio en sentido económico) ya que se trata de "actividades desarrolladas por entidades estatales (solución de principio) o por su mandato expreso" (solución de excepción efectivizada a través de concesiones). Aunque no es este el lugar para profundizar en la distinción entre monopolio y exclusividad (22), lo cierto es que ambos conceptos traducen la supresión de la libre competencia. Sin embargo, mientras que el concepto de monopolio se asocia a la actividad estatal en el campo de los servicios de libre prestación, la noción de exclusividad se vincula a la exclusión de otros prestadores ya que la "publicatio" del servicio apareja su exclusión del campo de la libertad de los particulares.

Las restricciones propias del régimen clásico de los servicios públicos -económicamente monopólicos, de mínimos, uniformes- aparejaron su crisis actual (23) y el afloramiento del llamado "nuevo modelo de servicios públicos competitivos" (24). En particular, como consecuencia de la antes descripta realidad impuesta por el desarrollo de la telemática, en los últimos años ha venido acuñándose la noción de servicio universal a su respecto, especialmente en los países de la Unión Europea (25).

Es que la evolución tecnológica reciente ha dado lugar a la multiplicación de servicios, cuyo disfrute por todos los ciudadanos debe ser garantizada sobre la base de principios como la no discriminación o la transparencia. Ello ha llevado a destacar la necesidad de definir el servicio universal como uno de los elementos básicos de la sociedad de la información (26), siendo sus elementos claves los siguientes: campo de aplicación, métodos para el cálculo de costos, y posibles mecanismos para distribuir toda carga asociada al servicio universal (ya que éste obliga a proporcionar acceso al mismo a un precio asequible a todo usuario potencial).

La distinción entre las prestaciones de mercado y las prestaciones de servicio universal se funda en que estas últimas son modalidades a las que el mercado, por sí solo, no daría respuesta y la autoridad entiende que deben ser cubiertas porque constituyen un estándar mínimo al que todos tienen derecho. Así, la apertura de los servicios a la competencia y a las leyes de mercado (frente a la idea tradicional de que todo servicio público, como actividad reservada, confiere exclusividad), se caracteriza básicamente por las siguientes notas (27):

a) la no calificación como servicio público de una actividad o sector en su conjunto sino sólo de algunas tareas o actuaciones concretas dentro de aquél, de modo que, en lugar de declarar servicio público a las telecomunicaciones, lo que hay que hacer es precisar cuáles son las obligaciones o cargas de servicio universal que hay que garantizar a todos (lo que exige la diferenciación de prestaciones tales como el servicio de telefonía básica y los servicios de valor agregado);

b) el abandono del concepto de reserva, con todo el régimen jurídico que este concepto lleva consigo (de titularidad de la actividad a favor del Estado, de la concesión como transferencia, etc.); y

c) la sustitución de un régimen cerrado (de exclusividad) por un régimen abierto a la entrada en el sector, bajo un sistema de autorización reglamentada y de imposición (unilateral o contractual) de cargas u obligaciones destinadas a garantizar determinadas prestaciones al público, que se impondrán de modo vinculante a todos cuantos actúen en el sector (con la consiguiente compensación económica).

---

(22) Ver: Carlos E. DELPIAZZO - "Manual de Contratación Administrativa" (Montevideo, 1993), tomo II, pág. 93 y sigtes.

(23) Héctor A. MAIRAL - "La ideología del servicio público", en Rev. de Derecho Administrativo (Buenos Aires, 1993), Año 5, Nº 14, pág. 359 y sigtes.

(24) Gaspar ARIÑO ORTIZ y otros - "El nuevo servicio público" (Marcial Pons, Madrid, 1997), pág. 25 y sigtes.

(25) Ives POULLET y otros - "Servicio universal público en la política europea de telecomunicaciones", en Informática y Derecho (Mérida, 1996), Nº 12-15, pág. 827 y sigtes.

(26) Gemma GARCIA PELAYO - "Las telecomunicaciones y la sociedad de la información en la Unión Europea", en Derecho de las Telecomunicaciones cit., págs. 299 y 300.

(27) Gaspar ARIÑO ORTIZ - "Servicio público y servicio universal en las telecomunicaciones", en Derecho de las Telecomunicaciones cit., pág. 761 y sigtes.; y "El nuevo servicio público" cit., pág. 31 y sigtes.

La Unión Europea se ha pronunciado con bastante precisión sobre las características del servicio universal, el cual, no sólo hay que establecerlo y financiarlo sino concretarlo y mantenerlo actualizado al compás del devenir tecnológico [28].

IV) IMPACTO DE LA CONVERGENCIA EN LO ORGANIZACIONAL

En el ámbito interno de cada Estado, una de las peculiaridades de la actual regulación para la competencia [29], constitutiva de lo que se ha llamado el Derecho de la regulación económica [30] y que es evidente en el ámbito de las telecomunicaciones y la informática convergentes, es la transformación de las Administraciones públicas en su organización y en su quehacer.

Desde el punto de vista organizativo, es imprescindible la separación de las actividades regulatoria y prestacional [31] y la consiguiente aparición de órganos o entes reguladores independientes [32].

En el campo de la telemática, ello es particularmente importante por tratarse de un sector donde la competencia puede verse muy condicionada por el papel fundamental que desempeñan las redes. La existencia de un regulador independiente -al estilo de la Oficina de Telecomunicaciones británica (OFTEL) o de la Comisión Federal de Comunicaciones (FCC) estadounidense- permite el desarrollo de un sistema eficiente, donde ninguna compañía operadora puede abusar fácilmente de su posición dominante y donde se favorece la entrada de nuevos operadores [33].

En lo que refiere al nuevo papel de la Administración, ésta es responsable de establecer la orientación básica del sector, poniendo especial cuidado en la cobertura de las obligaciones de servicio universal. En cambio, recae sobre la iniciativa privada el desarrollo de la actividad prestacional, aunque bajo supervisión de la autoridad pública, a la cual compete especialmente [34]:

a) la supervisión del cumplimiento de las condiciones bajo las cuales actúan los distintos operadores;

b) el control sobre la calidad de las infraestructuras y de los servicios;

c) la garantía de confidencialidad o privacidad de las comunicaciones;

d) la protección de los derechos de la propiedad intelectual; y

e) el control de algunos contenidos que puedan resultar contrarios al interés público en el tráfico de información en el ciberespacio (como es el caso de la ley estadounidense de 8 de febrero de 1996 respecto a la circulación de información pornográfica accesible a los menores).

---

(28) Gaspar ARIÑO ORTIZ - "Servicio público y servicio universal en las telecomunicaciones", en Derecho de las Telecomunicaciones cit., pág. 767 y sigtes. y 773 y sigtes.

(29) Gaspar ARIÑO ORTIZ - "La regulación económica" (Abaco, Buenos Aires, 1996), pag. 73 y sigtes.

(30) Mariano R. BRITO y Carlos E. DELPIAZZO - "Derecho Administrativo de la Regulación Económica" (U.M., Montevideo, 1998), pág. 53 y sigtes.

(31) Juan Carlos CASSAGNE - "Los nuevos entes regulatorios", en Rev. de Derecho Administrativo, Año 5, Nº 14, pág. 485 y sigtes.

(32) Ismael MATA - "Los entes reguladores de los servicios públicos", en El Derecho Administrativo Argentino Hoy (Edit. Ciencias de la Administración, Buenos Aires, 1996), pág. 119 y sigtes.; y Julio R. COMADIRA - "Derecho Administrativo (Abeledo Perrot, Buenos Aires, 1996), pág. 217 y sigtes.

(33) Laureano LOPEZ RODO - "La Administración pública y las telecomunicaciones", en Derecho de las Telecomunicaciones cit., pág. 634 y sigtes.

(34) Laureano LOPEZ RODO - "La Administración pública y las telecomunicaciones", en Derecho de las Telecomunicaciones cit., pág. 631 y sigtes.

Los principales retos a afrontar por el nuevo modelo tienen que ver principalmente con tres aspectos [35]:

a) el estatuto de los operadores y su número;

b) la forma de atender el servicio universal (con especial referencia a la cuestión tarifaria); y

c) la interconexión de los servicios.

Por otra parte, en el ámbito internacional, es posible señalar la creciente cooperación y la búsqueda de nuevas formas organizativas y de articulación, imprescindibles frente al desborde tecnológico [36].

V) CONCLUSION

Sin que puedan alcanzarse todavía conclusiones definitivas, parece claro que la convergencia de la Informática y las Telecomunicaciones, con su impacto en la prestación y organización de los servicios telemáticos, permiten augurar un amplio cauce de desarrollo de este nuevo Derecho al que, por comodidad de lenguaje, podemos llamar Derecho Telemático.

Aún cuando el mismo no goza todavía de una madurez académica y de una institucionalización suficiente, la necesidad y conveniencia de encarar su estudio científico en forma sistemática es indiscutible.

A ello deberán dirigirse buena parte de los esfuerzos jurídicos del porvenir inmediato.

---

[35] Tomás DE LA QUADRA SALCEDO - "Telecomunicaciones y Derecho público", en Derecho de las Telecomunicaciones cit., pág. 144 y sigtes.

[36] Félix FERNANDEZ SHAW - "Organización internacional de las telecomunicaciones y de la radiodifusión" (Tecnos, Madrid, 1978), pág. 23 y sigtes.; y "Cuaderno de bitácora de las telecomunicaciones", en Derecho de las Telecomunicaciones cit., pág. 151 y sigtes.

"Contenidos y Censura en Internet. Críticas al Proyecto de Ley de Chile, de agosto de 1999"

Renato Javier Jijena Leiva (Chile)
Abogado
Profesor de Derecho Informático UGM
Diplomado en Derecho Informático - Universidad de Zaragoza Chile

renatojijena@entelchile.net
rjijena@ucv.cl

I. INTRODUCCION.

El 31 de Agosto de 1999 un grupo de Diputados ha sometido a trámite parlamentario una moción legislativa de tan sólo cinco artículos -en adelante la MOCIÓN- sobre ***"Regulación de Internet"***, contenida en el ***Boletín N°2395-19***. Se trata de un hecho que esperamos nunca ocurriera en Chile, menos en la forma errada en que se pretenden incorporar al ordenamiento jurídico normas que, como demostraremos, en la práctica serán inoperantes frente a la realidad internacional de Internet y que importan un fuerte grado de censura y un atentado a la libertad de expresión.

En el acápite II se consignan diversos conceptos sobre el tema de las sociedades de la información y las redes telemáticas, sean estas cerradas o abiertas como Internet.

En el acápite III se enuncian los ámbitos más importantes de la relación entre el derecho e Internet, se señalan de manera general los obstáculos o las circunstancias que explican que es de la esencia de la red su "aterritorialidad" y la inconveniencia o improcedencia de su regulación legal a nivel de un solo Estado, se critican anteriores y errados intentos censuradores de otros Diputados y se reivindican como mecanismos de solución frente al problema de los contenidos ilícitos de Internet los tratados, la autorregulación y los mecanismos técnicos.

En el acápite IV se centra el análisis precisamente en el problema de los contenidos ilícitos de la red, en esencia un asunto de optar entre la libertad de expresión y las iniciativas de censura, y se hace referencia a iniciativas del Derecho Comparado, en especial aquellas como la *"Decency Act"* propuesta para EE.UU. que en 1997 fue declarada inconstitucional.

Recogiendo las propuestas y elementos anteriores, en el capítulo V del informe se analiza el Boletín N°2395-19 y en el acápite VI se formulan algunas consideraciones finales.

II. INTERNET, DERECHO Y FACTIBILIDAD DE REGULACION LEGAL.

1. Limitantes u obstáculos jurídicos.

Antes de analizar desde la perspectiva de la ciencia jurídica temas como el de la eventual regulación legal de los contenidos ilícitos de Internet, hay que entender que para abordar la problemática de la red, imaginaria -y geográficamente- debemos situarnos en el lugar físico o en el país donde esté instalado un servidor computacional que provea dichos contenidos (cosa que tecnológicamente puede no ser tan fácil de determinar). No hay que atender al Estado o país en que estén ubicados los usuarios-navegantes de la red, porque éstos, telemáticamente y a través del ciberespacio lo que hacen es llegar hasta o acceder a ese determinado servidor y a las páginas con diversos contenidos (los menos son los ilícitos) que en él se mantienen, porque ellos lo desean así y porque libremente han optado por acceder a dichos sitios, acción virtual que tecnológicamente se materializa porque varios ISP o proveedores de conectividad lo posibilitan mundialmente.

Una idea es esencial, y ella no ha sido entendida por parlamentarios y abogados chilenos. Internet –una red telemática pública y abierta- descansa en su "no regulación" o "desregulación local", lo que implica que no se puede censurar desde un Estado determinado una realidad virtual que -normativamente y en teoría- sólo podría llegar a regularse mediante un tratado internacional, siempre y cuando existan criterios uniformes respecto a la forma de hacerlo, v.gr., respecto a la improcedencia de difundir contenidos pornográficos. Pero ocurre -es la realidad- que en países más liberales como Holanda la pornografía no es considerada ilegal, al menos no al nivel de países más conservadores como Chile.

Internet no respeta límites geográficos y no reconoce fronteras o jurisdicciones estatales[1]. Los canales de la red traspasan todas las fronteras geográficas y son "aterritoriales". Leyes como las chilenas -v.gr. de delitos contra la moral, de abusos de publicidad, de derechos del consumidor, de propiedad intelectual e industrial, etc.- sólo pueden pretender tener vigencia dentro del territorio de nuestro país y los tribunales no pueden aplicarlas en el extranjero porque carecen de Jurisdicción para hacerlo. En consecuencia, siempre existirá incertidumbre respecto de la ley aplicable a actos que carecen de localización física precisa.

2. Propuestas de solución.

Desde ya y antes de entrar en el análisis del tema de los contenidos ilícitos desde la perspectiva de garantías fundamentales como la libertad de expresión, dejamos senatdo que somos partidarios de evitar que Internet se transforme en un "gueto anárquico" donde no se apliquen las normas que rigen la convivencia en sociedad, y especialmente creemos importante instar por resguardar derechos como el *copyright* en el ciberespacio. Pero la restricción de derechos y el control público de actos ilícitos en el mundo virtual es difícil y no puede derivar en excesos desproporcionados e injustificados o en prácticas de censura.

Creemos que una solución jurídica descansa -teóricamente- en los **tratados internacionales[2] o leyes supranacionales** y en los **resguardos técnicos ya existentes como los software "filtros".** También deben considerarse como una opción jurídica viable las **modalidades de autoregulación.** Por su propio peso e importancia el desarrollo y los conflictos jurídicos en Internet pueden traducirse en el surgimiento de normativas que, impulsadas por algún país u organismo internacional, tengan acogida y sean aceptadas mundialmente por los usuarios de la red. Así ha ocurrido con la reglamentación desarrollada por la IANA[3] y la ICANN[4] en relación a la asignación de direcciones virtuales o de los nombres de dominio.

III. EL PROBLEMA DE LOS CONTENIDOS ILICITOS EN LA RED: ¿CENSURA O LIBERTAD DE EXPRESION?

1. El problema o la hipótesis de trabajo.

A través de Internet, a fin de cuentas una herramienta tecnológica o telemática, pueden transmitirse datos, documentos, imágenes y sonidos de diversa naturaleza o contenido, sean lícitos o ilícitos, morales o inmorales, permitidos o prohibidos, benignos o nocivos.[5] Esta es una característica de la esencia de la red que, salvo excepciones muy reguladas y justificadas como la comisión de delitos, no puede -y nunca debería- modificarse legalmente. Dicho de otra forma, lo que debe buscarse es un adecuado equilibrio entre esta garantía de la necesaria li-

---

[1] Cabe consignar que, premeditadamente, las direcciones virtuales o los nombres de dominio de Internet fueron pensados para ser geográficamente independientes.

[2] Al decir de Florencio Utreras en un texto base que preparó para los trabajos que en 1998 desarrolló una Comisión Nacional de Tecnologías de la Información, y anticipándonos al estudio de una problemática específica, "está claro que con el advenimiento de Internet el acatamiento de la ley de propiedad intelectual... requiere de un gran acuerdo internacional".

[3] La sigla corresponde a la Internet Assigned Numbers Authority, un organismo contratado por el Gobierno de EE.UU. para administrar técnicamente el sistema de direcciones o nombres de dominio en la red.

[4] La sigla corresponde a la Internet Corporation for Assigned Names and Numbers,

[5] Hay quienes distinguen entre "contenidos ilícitos" y "otros contenidos nocivos". Ejemplo de los primeros -que a nivel de cada Estado o localmente se consideran delitos- sería el acceso de los adultos a pornografía infantil, la trata de blancas o redes de prostitución, y la difusión de contenidos racistas; ejemplo de los segundos sería el acceso de niños a contenidos pornográficos para adultos.

bre circulación de la información -en definitiva un derecho tan fundamental como la libertad de expresión- y la protección del interés público, sin que existan a priori prácticas de censura arbitraria y abusiva[6-7]. Pero trazar una línea divisoria puede no ser tan fácil atendida la naturaleza y las características de Internet.

En definitiva, la cuestión se traduce en determinar si la difusión virtual de contenidos ilícitos es una conducta que puede dar lugar a que existan limitantes de alguna naturaleza (no necesariamente jurídicas) a la libertad de expresión, más no prácticas de censura arbitrarias o abusivas que atenten contra la esencia de Internet.

2. *Limitantes de jurisdicción.*

Frente al tema de la difusión o distribución de información de contenidos ilícitos, cada uno de los Estados en que estén instalados los servidores respectivos puede aplicar su legislación interna de delitos contra la moral, el orden público, la seguridad económica, la propiedad intelectual, la violación de secretos, etc. Pero ese Estado no puede pretender aplicar sus normas jurídicas más allá de los límites territoriales de su jurisdicción; existen excepciones, por ejemplo en materia de genocidio y delitos contra los derechos humanos, ...pero estas situaciones han sido calificadas previamente por la vía de acuerdos o tratados internacionales.

3. *La "Communications Decency Act" -CDA- de EE.UU.*

En cuanto a los contenidos de Internet ...válido es nunca olvidar lo que ocurrió con la llamada *"Communications Decency Act"* o Acta de Decencia de las Comunicaciones de EE.UU., promovida en 1995 por el senador Exon en el marco de la nueva ley de telecomunicaciones de ese país y ratificada como ley federal el 8 de Febrero de 1996.

En Junio de 1997 el Acta fue declarada atentatoria contra la libertad de expresión consagrada en la Primera Enmienda -y por ende inconstitucional- por la Corte Suprema de ese país, esencialmente porque se formuló de manera muy amplia o general al prohibir el acceso a sitios con "material (artículos y órganos sexuales o excretorios) considerado patentemente ofensivo e indecente" -un concepto demasiado ambiguo y vago[8]- a una persona menor de 18 años; más precisamente, se sancionaba con penas de hasta US$250.000 y dos años de cárcel a todo aquel que difundiera o colocara a disposición de menores de 18 años ilustraciones o textos patentemente ofensivos o indecentes en un foro *on line* de acceso público (léase redes abiertas). Específicamente las objeciones apuntaban a dos artículos de la Sección 502 de la CDA, los números 223(a)[9] y 223(d)[10].

Al igual que en Singapur, Vietnam o China[11], donde las restricciones se han transformado en política de Estado, o en Alemania -donde se han aplicado medidas parciales de censura que afectan a los ISP's-, la ley in-

---

6 El tema preocupa a una serie de organizaciones internacionales. En la dirección http://www.gilc.org/speech/un/gilc-udhr50-statement-es.html, por ejemplo, que es el sitio WEB de la Global Internet Liberty Campaign, se contiene una declaración en defensa de la libertad de expresión en Internet promulgada con ocasión del 50 Aniversario de la Declaración Universal de Derechos Humanos....

7 En un contexto más amplio que el del eje "libertad de expresión-interés público", y en consideración a los aspectos económicos involucrados y a la importancia comercial de la red, se ha visualizado el conflicto entre los intereses económicos y sociales de quienes desean promocionar el uso de Internet y la preocupación de los gobiernos que buscan defender la seguridad y evitar el uso de la red para el narcotráfico, el terrorismo o la pornografía infantil.

8 Véase lo dicho en la nota anterior, respecto a que la calificación de indecente para algún material o contenido de Internet es un concepto esencialmente variable entre una cultura y otra.

9 El artículo establecía que "...any person in interstate or foreign communications who by means of a telecommunications device, knowingly... makes, creates, or solicits and initiates the transmission of any comment, request, suggestion, proposal, image or other communication which is obscene or indecent, knowing that the recipient of the communications is under 18 years of age, shall be criminally fined or imprisoned..."

10 El artículo prohibía "...makes it a crime to use an interactive computer service to send or display in a manner available to a person under age 18, any comment, request, suggestion, proposal, image or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication".

11 El 30 de Diciembre de 1997 entro en vigencia en China un Reglamento de 25 artículos (cuyo texto original desconocemos), que estableció eventuales sanciones penales y multas, tanto para proveedores de acceso o ISP como para usuarios, que a través de Internet cometan diversos delitos configurados de manera demasiado ambigua y subjetiva, tales como: dividir al país y difamar a funcionarios y entidades del Gobierno (subversión política que realizan diversos movimientos separatistas y exiliados políticos); difundir información "considerada por el Gobierno de China como dañina"; revelar secretos de Estado; y, dinfundir material pornográfico y violento.

tentó coartar la libertad de expresión y sancionar también a los proveedores de acceso a la red, olvidando que los ISP no pueden determinar si un usario es o no menor de edad al momento de posibilitar el acceso a sitios con contenidos para adultos y que un gran porcentaje del material con contenido sexual explícito se origina o se emite fuera de los EE.UU.[12]

El 26 de Junio de 1997 por 7 votos contra 2 la Corte Suprema ratificó el dictamen federal de los jueces de Filadelfía y anuló las disposiciones de la ley, aplicando por primera vez a una red telemática mundial las disposiciones de la Primera Enmienda de la Constitución estadounidense, al igual que a la prensa y sin "reservas", ...y declarando inconstitucional dicha ley. El alto tribunal consideró que algunos de sus artículos claves efectivamente vulneraban el derecho a la libre expresión, e imponían severas restricciones a la difusión mediante Internet de materiales sexualmente explícitos a personas menores de 18 años, lo que equivalía a una censura ilegal por parte del gobierno del Presidente Bill Clinton. Al decir del Magistrado redactor del fallo de 40 fojas, Jhon Paul Stevens, *"...a pesar de la legitimidad y la importancia de la meta legislativa de proteger a la niñez de los materiales peligrosos, coincidimos en que el estatuto limita la libertad de expresión y en que el Gobierno no tiene la potestad para discriminar a los adultos con materiales que no sean aptos para niños"*.

5. LA SOLUCION TECNOLOGICA: LOS PROGRAMAS FILTRO, "CERROJO" O DE SELECCION DE CONTENIDOS, QUE BLOQUEAN EL ACCESO A DETERMINADOS SITIOS WE.

Creemos que el mecanismo más adecuado para evitar la existencia de contenidos ilícitos es la existencia de medios técnicos que, en la práctica, limiten o impidan el acceso sólo a dichos contenidos mas no a otros[13]. Si los usuarios pueden contar con programas que les permitan filtrar los contenidos, se hace plenamente factible permitir la libre circulación de la información reclamada por la libertad de expresión y el respeto a las preferencias personales, por ejemplo de los padres que quieran controlar el material a que acceden sus hijos. Por último, siempre serán mejores los filtros selectivos que las censuras generalizadas.

Existen tres tipos esenciales de programas filtro: los de ***lista negra***, que bloquean el acceso a determinados emplazamientos; los de ***lista blanca,*** que permiten el acceso a determinados sitios WEB autorizados expresamente y bloquean los restantes; y los de ***etiqueta neutra***, que asignan una etiqueta o valoración a los sitios y permiten que el usuario final decida su uso, clasifique o seleccione los contenidos y bloquee los que desee (son los filtros *PICS -Plataform for Internet Content Selection-* o Plataformas para la Selección de Contenidos en Internet). Entre los usuarios de la red a estos software se les llama *"Net Nanny"* o "niñeras para la red" y son de fácil adquisición en el mercado[14 -15].

Se trata de un nivel de censura o más bien de autocensura totalmente aceptable que, pragmáticamente, permite respetar la diferencia de criterios, valores o costumbres morales entre comunidades, países y culturas

---

12 Si bien es cierto una ley dictada en EE.UU. no podría haber afectado a todo el ciberespacio, lo que la hacía inefectiva al emitirse material indecente desde servidores úbicados allende las fronteras del país del Norte, por tratarse del Estado más interconectado del orbe una medida legal de censura habría sido imitada en otros países.

13 Así lo consignaron también los tres jueces federales del Distrito de Filadelfia, cuando en 1996 declararon inconstitucionales las disposiciones del Acta sobre Decencia de las Comunicaciones. En nuestra opinión, los programas filtro son la mjeor manera de permitir el uso de Internet sin que se comprometa la libertad de expresión.

14 Uno de los motores de búsqueda que ha asumido la taerea de posibilitar a sus usuarios objetar material indeseado es "AltaVista", de la empresa Compaq Computer Corp. A comienzos de 1999 desarrollaron el programa "AltaVista Family Filter", que mediante los recursos de chequear la categoría de las páginas WEB y del reconocimiento de imágenes, automáticamente filtra materiales objetables tales como violencia o pornografía.

15 Un grupo de compañías, entre las que se cuentan AOL Europa, British Telecommunications PLC, Cable & Wireless PLC, T-Online GmbH, Bertelsmann Foundation, Microsoft Corp. e IBM, constituyeron la Asociación de Calificación de Contenidos en Internet (Internet Content Rating Association o ICRA) para proteger a los menores y la libertad de expresión simultáneamente, dijeron las compañías en un comunicado. El sistema estará basado en el sistema de calificación de el Recreational Software Advisory Council (RSACi), que evalúa contenidos sexuales, violentos o lingüísticos en los software recreativos. La idea de ICRA es la autorregulación voluntaria, y propuso usar los mecanismos que ya utilizaban los navegadores Internet Explorer de Microsoft y Navigator de Netscape Communications Corp. La ICRA comenzó en abril de 1999 una ronda de consultas con organizaciones relacionadas con menores y consumidores, así como a otras partes interesadas, para desarrollar el sistema con el mayor respaldo posible.

diversas. Ya no hay eventual censura en la fuente o alguna restricción o prohibición legal, administrativa o judicial previa para publicar virtualmente determinados contenidos, sino que el control o filtrado se produce a nivel de usuario final en el computador donde se recibe la información.

V. ANALISIS DEL BOLETIN N°2395-19, SOBRE "REGULACION DE INTERNET".

A. Análisis de la presentación de la MOCIÓN.

1. Son acertadas y están bien expuestas en los fundamentos de la MOCIÓN todas las cuestiones relacionadas con el derecho de dar y recibir información, con las limitantes naturales al mismo -porque no es absoluto- y con el señalamiento de responsabilidades que deben hacerse efectiva eventualmente contra los "Medios de Comunicación Social". **El tema es que nada tienen que ver estas consideraciones con Internet.**

2. Se alude a "un sistema de medios de comunicación de masa" necesario para la existencia de una sociedad *democrática, pero no se entendió que no todos los "Medios de Comunicación de Masas" son* de aquellos "Medios de Comunicación Social" a que aluden la Constitución y las leyes. Internet se ha transformado en "el Medio de Comunicación de Masas por antonomasia", pero no es un "Medio de Comunicación Social" de aquellos en que existan editores o directores a los cuales responsabilizar de los contenidos informacionales o multimediales (datos, imágenes, videos) que navegan por la red.

B. Análisis del articulado propuesto.

1. El tenor de los tan sólo cinco artículos propuestos es el siguiente:

Artículo Primero: *El que difunda o propale a través de los sistemas, redes y procedimientos de Internet, o de otros servicios de igual naturaleza, informaciones, contenidos o noticias contrarias a la moral, el orden público, o las buenas costumbres será sancionado con una multa de 15 Unidades Tributarias Mensuales.*

Igual sanción se aplicará a quienes usen dolosamente tales servicios y redes con el propósito de incitar al odio y la discriminación contra grupo de personas en razón de su raza, nacionalidad, sexo o religión; y a los que utilicen esos servicios o redes para difundir pornografía o efectuar una apología de la violencia.

Artículo Segundo: *Será competente para conocer y fallar las causas a que diere lugar la aplicación de la norma anterior, el Juez de Policía Local correspondiente, el que aplicará el procedimiento a que se someten las causas bajo su juridicción.*

Artículo Tercero: *La autoridad respectiva tratará que en los programas de estudio de la enseñanza básica y media se contengan cursos destinados a enseñar la forma de utilizar las redes y servicios de internet o de otros servicios de igual naturaleza, con la finalidad de difundir la cultura.*

Artículo Cuarto: *El que para difundir sus servicios o programas a través de las redes de internet, utilicen procedimientos que engañen sobre el contenido verdadero de los programas o "Servicio", será sancionado con la pena establecida en el artículo primero.*

Artículo Quinto: *La correspondiente autoridad que tenga que ver con la materia, dará a conocer a la comunidad dentro del plazo de seis meses las técnicas idóneas que los usuarios de los servicios de internet pueden usar voluntariamente para filtrar o controlar el contenido de los programas difundidos a través de las redes señaladas.*

2. La crítica esencial que cabe hacer a todos los artículos es que por tratarse de normas legales que sólo podrán tener vigencia al interior de Chile en la práctica constituyen meras declaraciones de principios, fácilmente vulnerables por la aterritorialidad de Internet, salvo, como comentaremos, la eventual censura implícita que acarrearía la aprobación del artículo 1°.

3. Análisis del artículo 1°.

La norma alude a "el que" o "a quienes" mediante Internet difundan contenidos ilícitos o contrarios a la moral, el orden público y las buenas costumbres -conceptos jurídicos indeterminados que en teoría deberán perfilar los Jueces de Policía Local-, y que dolosamente realicen prácticas difamatorias o injuriantes.

Lo señalado se concibe como una infracción meramente administrativa cuya única sanción es una multa de 15 UTM. Si existe tanta preocupación, ¿porqué no instaron por la tipificación de figuras penales?.

Se trata de una mera declaración de principios fácilmente vulnerable contratando un espacio en un servidor ubicado fuera de Chile. Lo riesgoso, lo peligroso y la medida censuradora está en que los sujetos activos de las infracciones pueden ser cualquiera, todo el mundo, especialmente los ISP o proveedores de conectividad. Que duda cabe que estas empresas, enfrentadas a la posibilidad de ser sancionadas pecuniariamente, tendrán que filtrar e impedir el acceso de sus usuarios abonados a aquellos sitios WEB que -en su opinión- pudiesen ser considerados como contrarios al orden público, la moral y las buenas costumbres, e incluso tendrían que fiscalizar los e-mail que por su intermedio se transmitan. Esto es censura a la libertad de recibir información en Internet. Esta sería una práctica de tanta gravedad como la escucha clandestina de las conversaciones telefónicas, actualmente constitutivo de delito en Chile, y vulnera garantías fundamentales como el secreto y la inviolabilidad de la correspondencia.

4. Análisis del artículo 2°.

Difícil será determinar al *"Juzgado de Policía Local correspondiente"*, sobre todo cuando el 98% de los contenidos ilícitos que pueden encontrarse en Internet provienen desde fuera de Chile. A riesgo de parecer irónicos -correr el riesgo vale la pena, aunque la gente convenientemente piense lo contrario- y atendido el tenor de la MOCIÓN presentada, ¿si un servidor que provee acceso a sitios WEB con contenidos ilícitos está ubicado en Turquía, habría que entender que de obtenerse una sentencia condenatoria ante un Juzgado de Policía Local chileno debería tramitarse un *exequator* y exigir el cumplimiento de dicha sentencia (aplicar una multa) en un tribunal del mismo nivel de Estambul?.

5. Análisis del artículo 3°.

No se trata de un artículo propio de una norma legal. Es una mera recomendación para *"la autoridad"*.

6. Análisis del artículo 4° .

Establecer que podrán aplicarse multas cuando a través de Internet se realicen conductas de publicidad engañosa y, por cierto, sólo para el caso que quien oferte con engaño un producto lo haga contratando un espacio en un servidor ubicado en Chile, es un conflicto jurídico que está subsumido por la denominada Ley de Derechos del Consumidor. Se trata de una explicitación obvia frente a un problema de poca ocurrencia en Internet (el *e-commerce* virtual se caracteriza por la buena fe, por la inexistencia de juicios y por el cumplimiento de los acuerdos...).

7. Análisis del artículo 5°.

Frente a este artículo uno no puede sino rendirse y declararse derrotado. Para intentar entender qué se quiso decir con este artículo habría que organizar un seminario o un panel de debate. Reconocemos nuestra incapacidad para pensar en *"la correspondiente autoridad que tenga que ver con la materia"*. Nos rendimos.

Se habla de un plazo de seis meses para dar a conocer a la comunidad (¿nacional e internacional?) la existencia de técnicas idóneas de resguardo contra los contenidos ilícitos. ¿Seis meses contados desde cuando?. Establecer que una autoridad deba difundir la existencia de técnicas idóneas es un absurdo, toda vez que dichos recursos técnicos, sean software filtros o sistemas de encriptación, están disponibles en el mercado y en Internet, y es aquel, mediante las reglas de la oferta y la demanda, quien los provee. Se trata de una cuestión de hecho. Y si aparecieran nuevas "técnicas idóneas", ¿tendría que volver a informar a la comunidad?. Quisiéramos creer que los Diputados patrocinantes quizás estaban pensando en el tema de definir por ley el largo o la extensión en bits de los sistemas de encriptación, cuestión que ni siquiera EE.UU y la Unión Europea han podido aún conciliar...., pero cuesta creerlo.

El Riesgo u Oportunidad del MP3

Fredrick Vega Lozada (Puerto Rico)
Director del Departamento de Economia Universidad Interamericana de Puerto Rico

RECINTO METROPOLITANO . LL.M. UNIVERSIDAD DE STRATHCLYDE EN REINO UNIDO,
JURIS DOCTOR UNIVERSIDAD DE PUERTO RICO, M.B.A. LONG ISLAND UNIVERSITY, NEW YORK.
Nacionalidad: Puertorriqueño, ciudadano de Estados Unidos (EUA).
CALLE PECOS 1645 PARADISE HILLS
SAN JUAN, PUERTO RICO 00926
FAX: 787-250-0361
Fredrick@tld.net
fvlozada@inter.edu HTTP://WWW.METRO:INTER.EDU/

La internet en su máxima expresión, el World Wide Web (WWW) se ha encargado de revolucionar todos los esquemas socioeconómicos y culturales en nuestra comunidad internacional. Era cuestión de tiempo en que la expressión cultural más distintiva de nuestra América estuviera en asedio por una nueva tecnología; El MP3.

El MP3 es una tecnología de comprimir archivos que expone en forma de algoritmo la expresión a sintetizarse y luego llevarla a la internet y tenerla accessible a cualquiera en el mundo.

Esta investigación presentará la situación del MP3 y su alcance de riesgo y oportunidades en cuanto a nuestra música y nuestros artistas.

I. INTRODUCCION

La revolución tecnológica de la decada de los noventa impulsada por la internet representa uno de los acontecimientos más importante para la humanidad. La tecnología integrada al microprocesador unido al énfasis en promover proyectos socioeconómicos neoliberales dentro de reformas motivadas por revoluciones pacíficas hacia la democracia[1]. Ha desarrollado la convergencia de tecnologías de gran diversidad, aplicación y accesibilidad[2].

Todas las manifestaciones humanas han sido marcadas por esta nueva revolución tecnólogica, inclusive las artes[3].

Hay pinturas y serigrafías en medios eléctronicos. Los museos y galerías del mundo han sido partícipes de este arte ciberneticos. Sin embargo, la música parecia en cierto modo immune, solo las computadoras habían invadido el espacio de los músicos representando una sustitución laboral de músicos por programas de computadoras.

II. SITUACION DE LA MUSICA

La expresión cultural músical, se ha desarrollado en un increíble y en la mayor de la ocasiones injusto sistema de regalías que hace realmente oneroso la creación musical, especialmete en relación a nuestros países caribeños, repasémoslo.

---

1 · Theseus International Management Institute http://www.theseus.fr/
2 · Nicolas Miletitch. El Nuevo Día. Jueves 21 de enero de 1999. P.72.
3 · Richard Lacago. "The end of who World as we Know it ". Time Magazine. January 18, 1999. P. 72-78.

Cuando una banda de cumbia, reggae, salsa, soka, merengue hace una canción esta banda son los dueños de los derechos de autor sobre esta canción. Su casa disquera son los dueños de los derechos de la grabación de la canción. El derecho patrimonial remunerable sobre la canción grabada proviene sobre la venta de los derechos de autor cuyo esta se conoce como licencia de publicación. Hay cerca de ocho (8) formas de licencia de publicación aunque las más communes estos son: licencia mecánica, licencia de impresión, licencia de ejecución (Conciertos o Presentaciones) y de sincronización.

Teóricamente nadie debe de tocar la música de un compositor sin antes pagar por los derechos de licencia de ejecución que el compositor de música posee. El compositor tiene que recibir compensación económica cada vez que su composición se ejecuta en la radio. Hay empresas autorizadas para ofrecer el servicio de recolectar el dinero por el compositor[4].

Si alguien quiere grabar su canción tambien tiene que pagar por la licencia de reproducción. A su vez , si alguien quiere imprimir y utilizar su música para un comercial o filmación tiene que pagar una licencia de impresión o sincronización,respectivamente.

Es importante señalar que cada país establece atravez de las oficinas gubernamentales de Registro o Protección de Derechos de Autor las tarifas pertinentes para cada una de estas licencias.

Nuestros músicos en el mejor de los casos se encuentran en la desventajosa situación de contabilizar los recaudos esperados y generados por sus distintas licencias.

En ocasiones acuden a una agencia o empresa de publicaciones que "se encarga de recaudar el dinero por un porcentaje de hasta un 50% de los recaudos obtenidos de los derechos de autor de los compositores. En el peor de los casos algunas empresas disqueras pretenden quedarse con el derecho de licencias al contratar a bandas que estan iniciandose o desconocidas y esto trae que el artista músico pierda sus derechos.

Esta común situación que choca con los más sencillos criterios de razonabilidad se agrava en nuestros países caribeños donde los derechos de licencia de compositores no se ponen en vigor y en ocasiones son inexistentes o en su major caso limitados. Abundan casos de artistas talentosos jóvenes que son explotados[5] por las casas discográficas[6].

III. LA ERA DE LA INTERNET: EL MP3

La presentación en los mercados mundiales de la grabación audiodigital iniciada a mediados de los ochenta aumentó la piratería de música[7].

Una persona que quisiera grabar un cassette de música no tenía oportunidad de transmitir una grabación original a otro medio análogo sin la pérdida de calidad en la grabación. Por ejemplo, una grabación análoga en cassette o disco de vinil o de otro cassette o disco compacto tenía una reducción en la calidad de la músi-

4 · John C. Yates & Paul H. Arne. Between a Rock and Hard Place: How Software Companies can Soften the Blow of the New Millennium. July 14, 1998. Yvonne Perkins. Eve of the New Millennium: Year 2000 IBM Santa Teresa Laboratory- Culpeper Forum Presentation. July 1997. http://www.culpeper.com/y2k/articles.asp. Report of the New Zealand Government Administration Committee. The Y2K Inquiry into the year 2000 date coding problem. April 1998. http://www.year 2000.coNZ/y2Kgov. Los Sistemas de Información pueden fallar, otros sistemas pueden perder datos. Los Sistemas de Información pueden cometer errores en sus operaciones. Una Encuesta de la Empresa Time/CNN publicada el 18 de enero de 1999 p. 64. Sus resultados fueron que el 59% de los entrevistados creían que las computadoras fallarían. 53% que los bancos tendrían dificultades en sus operaciones. 38% habría motines y problemas sociales y un 9% que el mundo terminará.

5 · The best of the new technologies of 1999 Computer Shopper, Nov 1999 v19 i11 p114

6 · La empresa Peer Internacional, Brodacst Music Inc, American Society Composer, Authors and Publishers, SESAC.

7 · Russ Mitchell U.S. News & World Report August 2, 1999 v127 i4 p49.

ca. Esta grabación de "segunda generación" no era tán buena. Con la grabación digital esto cambio totalmente no hay reducción en la calidad de la música no importa el número de "generaciones posteriores" a la original que se realize. La grabación digital permite realizar cualquier copia sin perder calidad y por ende es el sistema favorito para los piratas de música.

Hasta hace poco la Internet no era un medio común para distribuir música la razón era muy fácil y clara los archivos de música son muy grandes para accesarlos desde la Internet. Por esta razón una canción infantile simple como "mambru se fue a la guerra..." tardaría horas en ser accesada por internet. Sin embargo, varios algoritmos complejos usados para comprimir información en la actualidad permiten que los archivos de musica digitales puedan ser transferidos y guardados con rápidez y confiabilidad. El más conocido y utilizado es el Motion Picture Expert Group-1 Audio Level 3 o MPEG-1 Audio Layer 3 conocido en el argot de Sistemas de Información cómo MP3.

El MP3 es el más popular de los algoritmos para comprimir en uso en la Internet. Al comprimir el audio permite reducir un archivo de sonido a una razón de 12 a uno sin que se pierda la calidad en el sonido[8]. En la actualidad el Mp3 a rebasado al "sexo" como la mayor palabra buscada en la Internet. La Federación Internacional de la Industria Fonográfica estima que se accesa de la Internet cerca de 3 millones de canciones al día.

La popularidad del MP3 se debe a que es un algoritmo para comprimir información no propietario o sin derechos de autor. Su uso es gratuito y esta disponible a todos. Este sistema en la actualidad permite que una hora de música pueda ser escuchada y grabada en una computadora en varios minutos.

Estos extraordinarios cambios tecnológicos tienen un efecto en principios devastador para el sistema de retribución de derechos de autor en la industria tradicional de la música que hemos examinado anteriormente.

Se alega que el uso pricipal del MP3 es en tráfico de grabaciones ilegales de música. A raíz de que los archivos de MP3 no tienen codificación que pueda identificar si los archivos comprimidos están protegidos por derechos de autor o no. En la actualidad existen varios direcciones en la red de internet con música digital que usted puede accesar y grabar de la Internet pero que no es legal[9] por no haber cumplido con el pago de derechos de autor y sus licencias[10].

En *Recording v. Diamond* caso radicado a los Tribunales de Justicia Federal en los Estados Unidos de Norteámerica (EUA) la Asociación de Industrias de Grabación y Alianza de Artistas y Companías de Grabación (RIAA , siglas en Inglés)[11] alegó que el producto que la empresa Diamond vende el tocador de música portable Río y que este promovía la distribución en la Internet de música con derecho de autor pero pirateada en formato digital. Esto reduciría las ventas de legales de música. RIAA presentó prueba en el Tribunal y estimó la pérdida por este concepto de distribución illegal en la Internet en $300 millones de dólares anuales en el 1999 solamente en EUA .

Sin embargo, el Tribunal de distrito federal el 22 de junio de 1999 reconoció y permitió la totalidad dsiponibildad de sistemas cómo el de Rio. Despúes de analizar cón profundiadad la Ley de grabaciones caseras[12] estableció que la ley al aplicarla a la situación en particular de el equipo de Rio era confusa y no era clara. Por lo que el Tribunal investigó la Intención legislative y concluyó que la programación de Sistemas de Información cómo el algoritmo de MP3 es una obra literaria y no es un objeto material de la ley. Además, de que las computadoras no son objetos de grabar música según establecidos en la legislación, por lo tanto. El tri-

---

8 · En Estados Unidos de Norteámerica (EUA) seis companies domina el 90 % de distribución de música.

9 · Management Information Service. http://mis.udel.edu/

10 · School of Information University of Berkerly. http://www.sims.berkerley.edu/

11 · Michelle Manafy pirates, do you COPY? EMedia Professional May 1999 v12 i5 p12

12 · @EE Times Online. (Aris Technologies and Solana Technology Development merge; Diamond Multimedia's Rio MP3 player wins a court battle) (Late News)(Company Business and Marketing)(Brief Article)
Electronic Engineering Times June 21, 1999 p8

bunal decidió que el equipo de Rio no le aplicaba la legislación y no violaba ninguna ley federal. El Impacto de esta decisión es extraordinario para la música.

Posibles Efectos Negativos de la Tecnología

- Impacto Negativo para nuestra música caribeña

Nuestra creación musical continuamente está plagada de problemas por la puesta en vigor de las tarifas de licencias de derecho de autor y su relación con las casa publicadoras a esto le sumamos el que libremente se pueden accesar por la Internet música de nuestros artistas sin el correspondiente pago por derechos de autor. Existen disponibles ilegalmente copias digitales de grabaciones[13] de el Gran Combo de Puerto Rico, Silvio Rodríguez, Ricky Martin, Luis Miguel, Bob Marley, Soda Estéreo, Enanitos Verdes, Elvis Crespo, Chayanne, Juan Luis Guerra y otros[14]. Se cita países cómo Ukrania, Bulgaria,como permisivos en establecer dentro de sus fronteras archivos ilegales de música.

2. Impacto Positivo en nuestra música latina

Es importante señalar que las ventas legales de música utilizando el MP3 y el libre accesso y distribución rápida de grabaciones de música a desarrollado casas disqueras, publicadoras[15] y dsitribuidoras que operan exclusivamente por Internet. Se espera que para el año 2002 se produzcan $1,400 mil mllones de dólares en ventas solamente en EUA[16].

Además, hay contínuos debates en cuanto a si la piratería de música por la Internet en realidad representa pérdidas señaladas en ventas de música digital legítima[17]. Músicos y compositores nuevos sin experiencia pueden poner a disposición del Universo[18] su arte para que este sea el juzgador de su talento. El abuso experimentando por nuestros artistas en el pasado donde los obligaban a realizar contratos desventajosos para los artistas para poder aseguara una distribución adecuada se resuelve con la distribución universal en la Internet[19].

Las cinco empresas más importantes en la música han establecido alinzas estrátegicas para lanzarse a la Internet.

IV. CONCLUSIONES Y RECOMENDACIONES

La internet como fuente ídonea de comunicación universal[20] representa una perenne incertidumbre[21] sobre infinidad de procesos y nuevas industrias en este caso del MP3 podemos resumir lo siguiente:

---

13 · Recording v. Diamond, http://laws.findlaw.com/9th/9856727.html.

14 · Audio Home Recording Act of 1992 , 17 U.S.C. Sections 1001 et seq.

15 · Sweet music for some — but not all: The Web offers up free tunes, and headaches. (Brian Robertson of the Canadian Recording Industry Association estimates that the industry is losing $1.5 billion annually to music piracy over the Internet) DANYLO HAWALESHKA.
Maclean's July 19, 1999 p33

16 · Ukraine Overtakes Bulgaria As Top Music-Piracy Nation. (Brief Article) JEFF CLARK-MEADS.
Billboard May 15, 1999 v111 i20 p96(1)

17 · Roll-your-own CDs roll on. (Internet music with MP3)(Brief Article)
The Economist (US) April 10, 1999 v351 i8114 p12(1).

18 · The Economist (US); May 8, 1999 v351 i8118 p63(1) The big five hit the web."...So how much money is this new business likely to generate? Industry analysts are bearish about the short term. Jupiter Communications sees online music sales in America at a mere $30m in 2002. Forrester Research estimates that revenue will only really take off in 2003, when it will reach $1.7 billion—about 7% of total music sales..".

19 · Además, se estima que el precio actual de la música digital refleja las posibles pérdidas. Lewis Kurlatzick & Jackeline E. Penino, The Audio Home Recording Act of 1992 and the formation of copyright policy , 45 Journal Copyright Society United States of A,merica 497 (1998).

20 · MP3.com Announces Strategic Alliance With Cinram InternationalMP3.com Licenses Proprietary Just-In-Time Technology to Cinram International As Part of Multi-Faceted Global AgreementSAN DIEGO, Nov. 4 /PRNewswire/

21 · JustOn Introduces LiveFile, the Industry's First One-Step File Publishing ServiceNew Feature Makes Publishing Files to the Web Easier Than Ever; Adds Free Web-based File Storage to Personal HomepagesPALO ALTO, Calif. Nov. 3 /PRNewswire/

- El MP3 representa un reto a la comunidad internacional para poder establece métodos en conjunto para reglamentar los derechos de autor en la música y otras expresiones más allá los acuerdos existentes.

- EL MP3 no agrava la situación existente[22] en cuanto a la falta de coordinación y puesta en vigor de los tratados de derecho de autor internacionales e interrregionales[23] hay nuevas tecnologías para proteger los derechos de Autor una de ellas es el International Standard Recording Code (ISRC)[24].

- El MP3 brinda nuevas oportunidades de distribución[25] de manera legal[26] a nuestros artistas caribeños desconocidos o que comienzan a descollar[27]

- Urge diseñar la implementación de tratados internacionales como el de la Convención de Berne referentes al nuevo derecho emergente cibernetico que aseguren la jurisdicción de los países miembros para lidiar y resover el problema de derechos de Autor, Marcas de Fábrica en la Internet.

22 . Ear training: a digital music primer. (describes the major technological innovations in digital music downloading and recording) Matt Richtel, Sara Robinson. The New York Times July 19, 1999 pC6(N) pC6(L) col 1 (20 col in)

23 .La adopción de los dos dígitos permaneció porque era costo eficiente, fue adoptado por otros programadores y hasta en las universidades. Chris Taylor. "The History and the Hype". Time Magazine. January 18, 1999. P. 72-73.. Billboard, Sep 20, 1997 v109 n38 p8(2) U.S. begins WIPO debate: c'right treaties mulled worldwide. (World Intellectual Property Organization's international copyright treaties) Bill Holland; Jeff Clark-Meads.

24 . You can't stop the music. (the music industry in Australia)(Industry Trend or Event)(Internet/Web/Online Service Information) Selina Mitchell. Australian Personal Computer August 1999 v20 i8 p68(9

25 . MP3.com to Give Its Artists $200,000; Promotion Called 'Payback for Playback'

26 . Desarrollado por RIAA y la Industria Fonográfica Internacional.

27 . Rather than stamp out MP3, music companies aim to develop a variety of secure audio formats to save the day. Computer Shopper August 1999 p287

28 . Rather than stamp out MP3, music companies aim to develop a variety of secure audio formats to save the day. (Industry Trend or Event) Barbara Krasnoff. Computer Shopper August 1999 p287 . U.K. Biz Gets Gov't Support On Copyright. Jeff Clark-meads. Billboard July 18, 1998 v110 n29 p1(1) Bus.Coll.: 110W4234

29 .MP3 Components Coming. Audio Oct 1999 v83 i9 p22 The MP3 revolution: getting with it; a user's guide to technology that makes listening to music as well as making it a new experience; with practice, just about anyone can do it. The New York Times July 18, 1999 s2 pAR29(N) pAR29(L) col 2

"Dominios y Marcas en Internet. El Reglamento del NIC.CL"

Renato Javier Jijena Leiva (Chile)
Abogado
Profesor de Derecho Informático UGM
Diplomado en Derecho Informático - Universidad de Zaragoza
Chile

renatojijena@entelchile.net
rjijena@ucv.cl

1. DOMINIOS, MARCAS E "IDENTIDAD EMPRESARIAL".

Los nombres de dominio son las direcciones que permiten ubicar sitios en Internet, a pesar de que detrás de cada dirección hay un número único (URL) o identificador IP que registran los ordenadores, y son esenciales para mantener cierto mínimo orden indispensable en el ciberespacio. Ellos, alfabetizados para facilitar su manejo y recordación poseen una o varias denominaciones particulares y una genérica o superior llamada de "top level" que va al final, y que puede ser geográfica o nacional (.cl para Chile, .fr para Francia, .es para España, etc.) o temática (.org para organizaciones, .net para las redes y .com para las comerciales). Así por ejemplo serán nombres de dominio los siguientes: "www.acti.cl"; "www.eanchile.cl", "www.ucv.cl"; "www.ompi.org"; etc.

Lo que se busca es identificar las diversas direcciones virtuales mediante dominios o nombres generalizados, que son geográficamente independientes o transnacionales, que tienen un valor de mercado o económico y que pueden además constituir una "marca" susceptible de aprovechamiento comercial. Por cierto, no se trata de asuntos de menor cuantía. Así por ejemplo el dominio "business.com" fue vendido recientemente por la suma de 7.5 millones de dólares, convirtiéndose así en el más costoso de la historia. Hasta hace poco estaba registrado a nombre de un empresario inglés que hace tres años lo había adquirido a su propietario original por la suma de 150.000 dólares.

El enfoque del tema ha cambiado. Ya no podemos visualizarlo como la mera identificación técnica de ordenadores interconectados, sino que se trata de que toda entidad, empresa o persona natural que quiera mantener una página WEB u ofrecer comercialmente sus productos en Internet pueda tener debidamente inscrita y resguardada la dirección virtual de su sitio. Recordado es el caso de un particular que presentó ante el Departamento de Ciencias de la Computación (DCC) de la Universidad de Chile una solicitud de registro, en orden a constituirse en asignatario o "propietario virtual" de 119 nombres de dominio en Internet. Dichos nombres individualizaban a entidades públicas y privadas, a Órganos del Estado y a entidades financieras, a personas jurídicas y a personas naturales, muchas de los cuales tenían registradas las marcas comerciales respectivas. El perjuicio era evidente: de haberse asignado los dominios aquellas no habrían podido instalar páginas "WEB" con sus marcas corporativas sin previamente negociar con el titular del registro.

La ley de Propiedad Industrial establece que el titular de una marca comercial es propietario de la misma y que se encuentra facultado para usarla en forma exclusiva. La lógica indica que dicho titular también tiene el derecho de propiedad sobre la marca proyectado en Internet o virtualmente, a pesar de la "aterritorialidad de la red", debiendo tener la primera opción para inscribir el dominio o dirección a su nombre. Pero tal facultad sólo podría alegarse y hacerse valer con facilidad en Chile y sólo respecto a la denominación de top level ".cl", atendida la vigencia territorial de la ley sobre propiedad industrial que, a priori, no podría pretender tener aplicación fuera de nuestro territorio jurisdiccional.

En definitiva, se trata de proteger lo que un abogado y una empresa especializada han denominado la "identidad empresarial" o la "identidad comercial" de una empresa, producto o servicio (www.papernet.cl), es-

to es, uno de los más importantes activos intelectuales que surge a partir de las distintas experiencias que los consumidores tienen para percibir y posicionar una marca. Efectivamente, como se afirma, los dominios son hoy portadores de la identidad comercial de toda empresa y tienen un valor estratégico, y en ellos puede cristalizar –digamos gran parte- del posicionamiento, prestigio y trayectoria de una organización.

2. LINEAMIENTOS DE LA IANA Y LA ICAAN.

La existencia de un ente que controle el sistema de asignación de nombres de dominio en Internet es un tema complicado. A instancias de la IANA o Internet Assigned Numbers Authority, un organismo contratado por el Gobierno de EE.UU. para administrar técnicamente el sistema de direcciones de la red y mantener un "Registro de Nombres de Dominio", en un comienzo países como EE.UU. declararon urbi et orbi ser partidarios de la autoregulación. Pero en la práctica y reteniéndose de facto un servicio de carácter internacional, se *cedió mediante un contrato de exclusividad a una empresa vinculada al Departamento de Defensa y a la CIA* - Network Solutions Incorporate- el monopolio para que se registren y asignen y para que se mantenga un control exclusivo de los dominios más extendidos o que identifican a la mayoría de los actores de Internet (aquellos con denominaciones de top level temática, .com, .net, y .org). Tal opción, contenida en un primer documento conocido como "Green Paper", fue resistida por grupos académicos y técnicos interesados y proveedores como la "Internet Society", quienes reclamaron la necesaria creación de una entidad sin fines de lucro que se hiciera cargo de la tarea.

La IANA preparó un segundo borrador de propuesta o "White Paper", en general relacionado con el comercio electrónico global y, en particular, sobre un nuevo modelo de administración de nombres de dominio en que el proceso de registro es competitivo y no monopólico para Network Solutions, porque se postuló crear siete nuevos dominios genéricos y temáticos que serían administrados por diversas empresas repartidas en distintos lugares del mundo. El documento, suscrito por varias entidades vinculadas a Internet bajo la legislación de Suiza, contempló además la creación de un nuevo ente coordinador global de consenso, sin fines de lucro y formado por entidades privadas conocido inicialmente como Comisión de Servicios Públicos de Internet y denominado en definitiva, en Octubre de 1998, como "Internet Corporation for Assigned Names and Numbers" o ICANN.

En Chile no se le ha tomado el peso al hecho de que la última cumbre mundial de la ICANN se realizó en nuestro país, sobre todo porque del resultado de sus trabajos y conferencias surgirá la fórmula para cambiar el actual sistema de manejo técnico que financia y controla EE.UU.

3. EL REGLAMENTO DEL NIC CHILE (WWW.NIC.CL).

Este tema ha dado pie a la existencia de un importante grado de regulación jurídica en la red, para ser más exactos –y esto es novedoso-, de autoregulación. Las reglamentaciones que ha elaborado la IANA en orden a mantener un "Registro de Nombres de Dominio" han sido acogidas internacionalmente en forma mayoritaria. Por cierto, también se ha sostenido con cierto fundamento que el sistema sea administrado en cada país por el mismo órgano encargado del registro de marcas y patentes comerciales, pero esto enfrenta al menos dos problemas: que existen dominios que se asignan y registran para tener vigencia en todo el mundo y por sobre los territorios jurisdiccionales geográficos (.org, .com, .net); y que conllevaría dictar nuevas leyes e inventar nuevos procedimientos administrativos para la asignación, el registro y para la solución de controversias - en desmedro del mecanismo del arbitraje que es, evidentemente, el más idóneo-.

Actualmente en Chile se asignan e inscriben los dominios ".cl" en un registro que administra el Departamento de Ciencias de a Computación (DCC) de la Universidad de Chile. Allí funciona el Centro de Información de Redes (en inglés NIC). El Reglamento elaborado al efecto es una normativa autoacordada o autoestablecida, que no ha sido promulgada en Chile por autoridad alguna y por ende no publicada en el Diario Oficial (no cabe presumirla legalmente conocida por todos), sino que es aceptada y acatada de hecho por los

usuarios de Internet. Jurídicamente esto es novedoso porque se trata de una voluntad colectiva que autónomamente acepta determinadas normas, aunque hay quienes sostienen que todo asignatario en definitiva lo que hace no es sino celebrar un contrato de prestación de servicios con el NIC respectivo.

En un principio no se estableció relación alguna con las marcas que registra el Ministerio de Economía, pero posteriormente se agregó al Reglamento una instancia de arbitraje obligatorio en el caso que dos personas o empresas reclamen un mismo nombre y se hubiera formulado oposición dentro de un plaz de 30 días, debiendo el mediador o el árbitro, necesariamente, considerar la existencia de "marca preexistente" al decidir quien tiene el mejor derecho de usar un dominio.

La última modificación realizada por el NIC permite a toda empresa o particular que se sienta perjudicado por la inscripción de un dominio, y que no haya podido oponerse dentro de los 30 días que establece el reglamento, "gatillar un arbitraje" –al decir del abogado Gonzalo Sanchez- para intentar la revocación de inscripciones de dominios abusivos. El plazo para iniciar un procedimiento de arbitraje para revocar un dominio es de tres años a contar de la inscripción del mismo.

4. EL CASO ONDAC.

Por la vía del Recurso de Protección, que es una acción cautelar que ampara determinadas garantías constitucionales frente a actos arbitrarios o ilegales, en 1998 una empresa proveedora de software -Ondac Chile Ltda.-, que había registrado previa y debidamente en el Ministerio de Economía la marca "Ondac", recurrió en contra de la Universidad de Chile por haberse registrado o asignado en el DCC el dominio "ondac.cl" a otra empresa que no tenía derechos preexistentes. El mecanismo constitucional se utilizó amparándose legalmente en la normativa de la ley de propiedad industrial y en la CPE. de 1980, ante la negativa del ente universitario de registrar o asignarle el nombre de dominio a la primera por haberlo solicitado previamente la segunda en conformidad al Reglamento ad hoc.

El recurso fue declarado sin lugar en la Corte de Apelaciones: a) debido a que el DCC sólo cumplió con la reglamentación vigente y el recurrente no formuló oposición en los plazos que contempla el Reglamento; b) a que, en opinión del Tribunal, al DCC no cabía exigirle al momento de asignar un dominio un juicio o pronunciamiento respecto del alcance de la protección que se le otorga a las marcas comerciales registradas (se habría arrogado una potestad jurisdiccional ajena); y, c) a que el conocimiento de este tema no era propio de un recurso de protección.

No obstante que el DCC nunca pretendió arbitrariamente perjudicar a la empresa Ondac, el criterio del Tribunal es errado y producto de un análisis meramente formal. La Corte no entró al fondo del asunto. En la especie no cabía desconocer la aplicación de la ley de propiedad industrial, ni la procedencia del recurso de protección para detener en Chile y preventivamente (sin perjuicio de hacer valer otros derechos o reclamar conforme a la ley de propiedad industrial) una conducta perjudicial y atentatoria contra la garantía constitucional del derecho de propiedad, máxime cuando el Reglamento no puede considerarse una "ley especial" sino que es una normativa autoacordada o autoestablecida que no ha sido promulgada por autoridad alguna y que, hasta antes de contemplar un mecanismo obligatorio de arbitraje, podía lesionar los derechos de los titulares de las marcas comerciales.

5. SANCION A LOS "CIBERCUATREROS".

En EE.UU. dos texanos registraron una larga lista de nombres de dominio que incluían la palabra "microsoft", específicamente los nombres "microsoftwindows.com" y "microsoftoffice.com"; posteriormente solicitaron entre 50 y 100.000 dólares a la transnacional del software. Microsoft accionó legalmente por haberse infringido las marcas comerciales de la empresa y confundido a los usuarios. A la luz de estas prácticas, el Congreso de Estados Unidos aprobó una ley que sanciona penalmente a todos aquellos que, dolosamente y sin te-

ner fundamento, intenten registrar como nombres de domino marcas comerciales pertenecientes o previamente inscritas por otras compañías. Esto será aplicable, por cierto, siempre y cuando el hecho doloso ocurra dentro de EE.UU.

El Reglamento del NIC chileno, como ya comentamos, también acaba de ser modificado para regular este tema, estableciéndose que serán acogidos los criterios de la ICANN que permiten revocar la inscripción de dominios cuando se compruebe que se realizaron de mala fe. Por ende, quedó sin efecto, por atentarse contra la tutela del derecho de marcas, la norma cerrada del Reglamento que establecía que una vez inscrito un nombre de dominio ya no podía acogerse otra solicitud de registro por el mismo simplemente por razones de plazos vencidos u oportunidad de oposición no aprovechada.

Se han presentado en nuestro país casos de personas que a través de Internet han registrado en EE.UU. nombres de dominios con las extensiones ".net", ".com" y ".org" relacionadas con empresas chilenas. Cualquier acción legal de reclamo sólo podría intentarse conforme a la legislación del país Norteamericano o la reglamentación de Network Solutions, porque es dentro de su territorio jurisdiccional donde se produce el hecho del registro. Que la magia de Internet permita presentar una solicitud y obtener un registro de dominio en el extranjero desde o sin moverse de Chile no significa, como han creído algunos abogados anclados al derecho tradicional, que sea factible interponer en nuestro país una acción de reclamo civil o penal en relación a hechos acaecidos fuera de nuestro territorio.

Lo anterior fue entendido por la empresa Chilnet S.A., que a fines de 1998 ganó en primera instancia una demanda interpuesta en EE.UU contra los representantes de una compañía israelita que inscribió a su nombre los dominios "chilnet.com" y "chilnet.net", en el administrador de los dominios ".com" y ".net" de EE.UU. A quien solicitó la inscripción de los dominios la empresa se le hizo presente que bajo el Domain Name Registration Agreement (www.internic.net/help/agreement.txt) tenía que basarse en las pláticas de disputas suscritas en el sitio WEB del administrador de dominios, conforme a las cuales debía traspasar las inscripciones a la empresa chilena. Ante la negativa se realizó una presentación formal, con lo cual se obtuvo que la entidad reguladora bloqueara la petición de registro de dominios hecha por la empresa israelita y acogiera la petición de detener o dejar en espera -retroactivamente- el uso de los mismos.

Sistema de los Nombres de Dominio en Chile

Humberto Carrasco Blanc (Chile)
Abogado
Post-título de Asesoría Jurídica de la Empresa
Director de Derecho. Org Chile
Secretario de la Asociación de Derecho e Informática de Chile
ADI-Chile

INTRODUCCION

Los nombres de dominio han adquirido una importancia trascendental en el desarrollo del intercambio de la información en todos sus niveles, ya sea, en el ámbito comercial, educacional, etc.

No se debe olvidar que Internet nace en un principio para cumplir fines militares, científicos o académicos y la forma de identificarse a través de este conjunto de computadoras se manifestaba a través de códigos numéricos. Posteriormente ante la proliferación de enlaces computacionales fue necesario crear un sistema que permitiera identificar con mayor facilidad a los distintos ordenadores y es de esta forma que nacen los nombres de dominio.

En la actualidad nadie discute la importancia de los nombres de dominio y la influencia que ejercen en al ámbito del comercio electrónico, de manera que han surgido diversos conflictos en materias de marcas comerciales (en todo caso, también se han producido conflictos con los derechos de la personalidad).

Debido a las diferentes ventajas que presenta Internet, aumenta constantemente el interés en tener una presencia activa en la Red, generando a su vez, un aumento en las solicitudes de nombres de dominio.

Existen dos grandes grupos de nombres de dominio (TLDs), unos sin base geográfica y otros que si la tienen. Entre los primeros encontramos los .com, .edu, .net, .mil, .org, .gov, mientras que en los segundos existen diversos nombres de dominio que serán diferentes de acuerdo al país en que se soliciten. Ej: .cl, .ar, .es, fr, etc..)

En todo caso, el presente trabajo se relaciona con el dominio territorial .cl y no se refiere a los dominios de carácter genérico.

A su vez, utilizaremos el esquema proporcionado por el Jurista español Javier Maestre[1] con el fin de entregar la información en la forma más didáctica posible.

1. SITUACION GENERAL SOBRE EL DOMINIO:

a) Grado de desarrollo y utilización del dominio.

El sistema de nombres de dominio chileno no se encuentra en mal pie. En la actualidad, al día 19 de enero del 2000 se han registrado 18.896 nombres de dominio .cl, mientras que en trámite se encuentran 2.865.[2] A nuestro juicio, creemos que la cantidad de dominios inscritos demuestra la existencia de un sistema relativamente eficiente en comparación con otros países. No debemos olvidar que en nuestro territorio no existe una gran población y es todavía incipiente el desarrollo de Internet en nuestras fronteras. (eso sin desconocer que en el último año Chile fue el país que tuvo un mayor crecimiento en cuanto al número de usuarios que se conectaron a Internet).

---

[1] JAVIER MAESTRE ha entregado un cuestionario en virtud del cual se debe elaborar un estudio de los nombres de dominio de distintos países en la lista de REDI. Nosotros nos hemos valido de ese cuestionario para construir esta ponencia.

[2] Esta información ha sido proporcionada directamente por el NIC Chile.

b) Se subdivide el dominio de forma territorial (USA) o por materias (.com, .net, etc) y forma y requisitos de adscripción al subdominio.

En Chile no se subdivide el nombre de dominio .cl y no se tiene conocimiento de alguna iniciativa en este sentido, al menos no por la entidad que administra los nombres de dominio en el país. Lo anterior, no significa que en el hecho no existan los subdominios y estos son creados por los propios dueños de un dominio .cl.

En síntesis, no existe por parte de la DCC (entidad que regula los dominios en Chile) una subdivisión de los nombres de dominio. Por lo anterior, los particulares son libres de crear los subdominios que deseen.

c) Carácter de la persona que registra el nombre de dominio y breve explicación de su régimen jurídico (especificar si es organismo Público, Universidad o empresa privada [con indicación si tiene consideración de Administración Pública].

El NIC-CHILE

En nuestro país, el registro de nombres del dominio CL, denominado **NIC CHILE** (Network Information Center Chile), es administrado por el DCC (Departamento de Ciencias de la Computación de la Universidad de Chile), entidad que entrega nombres de dominio de acuerdo a un reglamento que sigue los principios contenidos en RFC 1592 (Dominian Name System Structure and delegation). Sin embargo, no existe una consagración legal que regule los conflictos entre los nombres de dominio, sólo un sistema arbitral diseñado en el reglamento señalado.

A su vez, el departamento de Ciencias de la Computación es parte, como se puede desprender, de la Universidad de Chile, entidad que constituye una persona jurídica de derecho público. Por lo tanto, el DCC actúa en virtud de esta persona jurídica, pero como organismo independiente.

d) Posibilidad de considerar el registro de nombres de dominio como un servicio público y las consecuencias de ello.(Posibles problemas de competencia de jurisdicción en las acciones dirigidas frente al organismo registrador)

A nuestro juicio, la función del registro de nombres de dominio en Chile puede entenderse como de carácter privado y no constituye una función pública (aunque el asunto es discutido en algunos países como España) .

Este parece ser el criterio adoptado por la doctrina nacional al estimar que la relación que nace entre un solicitante de un nombre de dominio y el ente administrador constituye un contrato de adhesión. En efecto, dispone el abogado GULLERMO CAREY CLARO que "Es por eso que cuando se dice que se vende un dominio, en estricto rigor lo que se esta haciendo es vender ciertos derechos personales que emanan del contrato de adhesión con el DCC."[3]. Los abogados PATRICIO DE LA BARRA y DIEGO VALENZUELA expresan que "Sin perjuicio de lo anterior, a la fecha podemos señalar que existe amplio consenso en el sentido que la antes señalada declaración jurada que el solicitante firma y presenta ante NIC–CHILE constituye en definitiva un contrato de adhesión, en cuyo mérito el reglamento adquiere fuerza imperativa respecto del solicitante".[4]

El hecho de que nazca un vínculo de carácter privado, contractual, implica el nacimiento de una serie de obligaciones que no sólo tienen su origen en la autonomía de la voluntad, sino que también legal.

---

[3] CAREY CLARO GUILERMO, "Aspectos sobre la naturaleza de los nombres de Dominio en Chile", http://www.anfitrion.cl/actualidad/relacion/carey.html.

[4] DE LA BARRA PATRICIO y VALENZUELA DIEGO, "Reglamentación para el funcionamiento del registro de nombres del Dominio ".Cl"", http://www.anfitrion.cl/actualidad/relacion/barra.html

En este sentido, al constituir un contrato de adhesión creemos que es perfectamente aplicable la ley que establece las normas sobre los derechos de los consumidores N° 19.496.

El ser aplicable las normas de esta legislación al contrato de adhesión que se celebra con NIC-CHILE implica consecuencias que no han sido previstas. A modo ejemplificativo podemos señalar las siguientes:

1. - El artículo 23 del reglamento (que se entiende incorporado en el contrato) señala que: "La presente Reglamentación podrá ser modificada o reemplazada las veces que sea necesario, a sólo juicio de NIC Chile, quedando obligado desde ya el usuario a acatar de inmediato las nuevas normas que se fijen, sin reservas de ninguna naturaleza."

Por otra parte dispone el artículo 16 letra a) de la ley 19.496 que " No producirán efecto alguno las cláusulas o estipulaciones que:

a) Otorguen a una de las partes la facultad de dejar sin efecto o ***modificar*** a su sólo arbitrio el contrato o de suspender unilateralmente su ejecución,....."

Si estimamos que se aplica la normativa, esta cláusula del reglamento no tendría aplicación respecto de los contratos de servicios de dominios que se encuentren vigentes y sólo sería aplicable a las futuras solicitudes.

2. - El artículo 6 del reglamento establece en su tercer punto que "Por el hecho de solicitar la inscripción de un nombre de dominio bajo el Dominio CL, se entiende que el solicitante:

- libera de cualquier responsabilidad a la Universidad de Chile, al Departamento de Ciencias de la Computación, a NIC Chile y a sus funcionarios y asesores, por las obligaciones, responsabilidades y otros actos o hechos que le generen obligaciones al solicitante, renunciando expresa y anticipadamente a las acciones legales."

Sin embargo, el artículo 16 dispone en su letra e) que "No producirán efecto alguno en los contratos de adhesión las cláusulas o estipulaciones que:

e) Contengan limitaciones absolutas de responsabilidad frente al consumidor que puedan privar a éste de su derecho a resarcimiento frente a deficiencias que afecten la utilidad o finalidad esencial del *producto o servicio, y."*

Por lo tanto, de seguirse aplicando el criterio del contrato de adhesión esta norma no tendría aplicación, por lo menos respecto de aquellos que la ley considera consumidores y cuyos actos sean civiles.

Existen otras situaciones en las cuales puede haber contradicción, pero que no mencionaremos por escapar a la finalidad de esta obra.

e) Intervención en la gestión del dominio, en alguna medida, de organismos con competencias en materia de marcas.

En nuestro país, el Departamento de Propiedad Industrial del Ministerio de Economía, Fomento y reconstrucción (http://www.minecon.cl/dpi/) es el organismo al que compete el otorgamiento de los títulos y demás servicios relativos a la propiedad industrial, pero no tiene ninguna injerencia en el otorgamiento de los dominios .cl que sólo están a cargo del NIC - CHILE.

2. SITUACION DE LAS NORMAS

a) Existencia de normas de registro de nombres de dominio.

Para el registro de nombres de dominio .cl, como se ha expresado, existe un reglamento que ha dictado NIC - CHILE. Estas normas, a nuestro criterio, tienen un carácter flexible en oposición a las restrictivas que existen en otros países. Este reglamento se puede consultar en: http://www.nic.cl/reglamento.html

b) Carácter que presentan las normas (¿Integradas en el sistema ordinario de producción normativa del Estado?)

Estas normas tienen su origen en la esfera privada y escapa al ámbito tradicional de producción normativa. No es el legislador, ni el poder ejecutivo u otro organismo administrativo el encargado de la elaboración de dichas normas. En efecto, las normas de registro de dominios nacen del DCC, organismo que las plasma a través de un reglamento y sus anexos.

c) Existencia de previsión de normas en caso de conflicto. El sistema empleado y el sometimiento al mismo (voluntario o preceptivo).

En nuestro país, el reglamento contiene dos sistemas de solución de conflictos. Uno de arbitraje y otro de mediación, este último método fue incorporado en virtud de una modificación de diciembre del año 1999.

1.- ¿Cuándo nace el proceso de mediación y arbitraje como mecanismo de solución de conflictos?

Es importante señalar que tanto la mediación, como el arbitraje nacen, por regla general, de un mismo hecho: Si existen dos o más solicitantes de un mismo nombre de dominio, esto es lo que Gabriela Paiva denomina "solicitud competitiva"[5], ya que existe una solicitud idéntica que compite con otra. De conformidad al artículo 10[6] del reglamento el NIC - CHILE mantendrá una lista de solicitudes en trámite y dentro del plazo de 30 días desde su publicación, los que se sientan afectados por dicha petición podrán solicitar ese mismo nombre de dominio dando origen al sistema de mediación y arbitraje.

Sin embargo, no es el único caso en que se da nacimiento a este procedimiento, sino que el artículo 14 establece otro, el cual se produce cuando una inscripción contraría las normas vigentes sobre abusos de publicidad, los principios de la competencia leal y de la ética mercantil, como asimismo, derechos válidamente adquiridos por terceros. En esta situación, el nacimiento de este proceso no es obligatorio sino que depende del NIC - CHILE.

Otro caso se presenta cuando se solicita la revocación de un nombre de dominio, según lo preceptua el artículo 21 del reglamento.[7]

Es interesante destacar como una de las características de este procedimiento, la validez de las notificaciones electrónicas para dar aviso de la existencia de un conflicto en torno a un nombre de dominio.[8]

---

5 PAIVA GABRIELA, "El Arbitraje como medio de solución de conflictos en la Internet", http://www.anfitrion.cl/actualidad/relacion/paiva.html

6 El artículo 10 dispone: "Una vez que la solicitud haya sido recibida por NIC Chile éste la publicará dentro del plazo más breve que sea técnicamente factible, y en todo caso dentro de los siguientes tres días hábiles, en una lista de solicitudes en trámite. Dicha solicitud se mantendrá en esta lista por el plazo de 30 días corridos a contar de la publicación, objeto de que eventuales interesados tomen conocimiento y, si se estimaren afectados, puedan presentar sus propias solicitudes para ese nombre de dominio."

7 Artículo 21 dispone que: "Para los efectos de solicitar la revocación de un dominio inscrito, será necesario que el reclamante:
a. solicite a NIC Chile por escrito, la revocación de dicho dominio, indicando los argumentos en que se funda, y
b. consigne la tarifa correspondiente al examen de admisibilidad, a nombre del árbitro que NIC Chile designe para la realización de dicho examen.
Recibida la solicitud de revocación, NIC Chile designará un árbitro de la nómina del turno, quien efectuará un examen de admisibilidad respecto de la solicitud. Efectuada la consignación para los efectos de este examen, a nombre del árbitro designado, NIC Chile le enviará los antecedentes para su análisis.
Si producto de dicho examen resultare admitida a tramitación la solicitud de revocación, NIC Chile notificará de ésta a las partes involucradas, via correo electrónico. La tramitación de una solicitud de revocación se sujetará a las reglas del procedimiento de MEDIACIÓN Y ARBITRAJE."

8 Son numerosas las normas que hacen referencia por un lado a la exigencia de que en las respectivas solicitudes se debe indicar el correo electrónico y que las notificaciones se harán por esta vía. Véase artículos 15, 16, 21 y artículo 2 del anexo número 1 del reglamento.

2.- ¿En qué consiste la mediación?

La mediación surge como una real alternativa de solución frente a un sistema más dilatado como es el arbitraje. La experiencia enseña que no en pocas ocasiones las partes al primer contacto que tenían, lograban ponerse de acuerdo en la forma de solucionar los respectivos conflictos y es por ello que a finales del año 1999 se introdujo esta modificación para agilizar los problemas derivados de los nombres de dominio.

A nuestro entender, este procedimiento de mediación es similar a la conciliación que regula nuestro Código de Procedimiento Civil en lo relativo a su finalidad, la cual es evitar un juicio innecesario ante un eventual acuerdo de las partes.

Cuando se origina el procedimiento de mediación, se insta a lograr acuerdos a través de mediadores que proporciona el propio NIC - CHILE. Lo interesante del sistema es que la designación de los mediadores no tiene costo para las partes. Es necesaria una audiencia a la que se cita a las partes vía correo electrónico y en ella se levanta un acta de todo lo obrado y deben las partes concurrir personalmente, aunque en ciertos casos se admite la comparecencia vía tele-conferencia. En el caso de que una de las partes no concurra a la audiencia se entenderá que no se ha logrado acuerdo.[9]

3.- En cuanto al Arbitraje

Si en el procedimiento de mediación no se lograre un acuerdo, se preguntará en esa misma audiencia, si fuere procedente, la posibilidad de que designen un árbitro de común acuerdo. En caso que sólo hubiere asistido una parte, se le indicará que puede tachar hasta tres árbitros de la lista respectiva y aquella parte no asistente se le otorgará un plazo de 10 días para hacerlo[10].

Es necesario señalar, que hubiere o no tachas se procederá a designar a un árbitro de la lista y de conformidad a las normas que el mismo reglamento establece para el turno.

El arbitro que interviene en este procedimiento tiene el carácter de arbitrador y tiene este carácter porque es la mejor forma de poder solucionar los conflictos que se generan en torno a los nombres de dominio. Las particularidades de Internet y un conocimiento técnico suficiente, hacen que el arbitro arbitrador sea el camino más expedito para una solución adecuada y rápida de la materia objeto de controversia. En síntesis, para que exista un procedimiento de arbitraje es necesario que se cumplan los siguientes supuestos:

a) Que estemos en presencia de aquellas situaciones que dan origen a un arbitraje y que hemos tratado con anterioridad.

b) Pago de Tarifa respectiva y la entrega de los documentos exigidos (artículo 12).

c) Elección o designación de un árbitro.

Las demás normas que regulan la materia no serán tratadas en esta oportunidad por no ser objeto de esta ponencia, pero se podrán encontrar en el reglamento antedicho.

4.- Cláusula que impone el sistema de arbitraje.

---

9 En al artículo 2 del anexo 1 se encuentran detalladas las normas sobre este tema.

10 El arbitraje se encuentra regulado en los artículo 3° y siguientes del anexo 1 del reglamento.
Artículo 7° del reglamento señala que "Podrán solicitar inscripción de nombres de dominios bajo el Dominio CL las siguientes personas:
c. Personas naturales actualmente domiciliadas o legalmente avecindadas en la República de Chile.
d. Personas Jurídicas Públicas o Privadas, Corporaciones y entidades de Derecho Público o Privado constituidas en Chile o debidamente autorizadas para operar en Chile."

Se debe señalar que no es posible al solicitante de un nombre de dominio discutir la norma que lo compele a aceptar el sistema de arbitraje. Sin embargo, resulta curioso que las distintas partes que pudieren estar involucradas se someten a un mismo arbitraje en virtud de diferentes contratos de adhesión.

d) Grado de apertura de las normas, con expresión de las principales limitaciones, en su caso, al registro de nombres (¿pueden residentes en otros países registrar nombres de dominio? ¿Puede una persona registrar).

Creemos que una de las principales virtudes de la reglamentación que estamos analizando es que no es restrictiva y todo lo contrario, facilita la obtención de los nombres de dominio y las soluciones a los conflictos potenciales. A pesar, que siempre van apareciendo situaciones novedosas que no se encuentran reguladas en el reglamento, felicitamos el esfuerzo del NIC -CHILE por incorporar actualizaciones en la forma más rápida posible. Un ejemplo de ello lo constituye la última modificación de Diciembre en que se adoptan (sin que fuera obligatorio hacerlo) las normas que al efecto dictó ICANN relativas al "Cybersquatting" o Ciberocupación en el mes de octubre del año1999:

1. - *¿Quiénes pueden registrar nombres de dominio en Chile?*

En nuestro país pueden registrar nombres de dominio tanto personas naturales como personas jurídicas, pero ambas deben tener residencia en el territorio Chileno.[11]

Nuestro país no restringe, a diferencia de lo que ocurre en España, la solicitud de nombres de dominio para personas naturales y ello no ha significado inconvenientes en la gestión de dominios en Chile.

2. - ¿Pueden los solicitantes ser titulares de más de un nombre de dominio?

No existe inconveniente en que una misma persona, natural o jurídica sea titular de más un nombre de dominio. Si bien esta facultad ha producido abusos en cuanto a aquellas personas que de mala fe se dedican al registro de nombres de dominio, ha permitido una flexibilidad adecuada a los requerimientos actuales. Además en virtud, de las recientes modificaciones se entregan herramientas suficientes para detener las actividades de los ciberocupadores, sin mermar la libertad de la solicitud de nombres de dominio.

Se debe destacar que con fecha 24 de noviembre de 1999 el NIC estableció una limitación a la solicitud de nombres de dominio por razones de conveniencia del sistema. En la actualidad sólo pueden solicitarse hasta 10 nombres de dominio sin que se haya pagado la tasa correspondiente.[12]

3.- ¿Es necesario tener residencia en Chile para ser titular de un nombre de dominio?

Podemos señalar que, en términos generales, es necesario que los solicitantes de nombres de dominio en Chile deben tener residencia en el territorio nacional. En todo caso, esto no significa que los extranjeros no puedan ser titulares de nombres de dominio .cl, ya que ellos pueden solicitarlos a través de personas que si tengan residencia nacional.[13]

e) Exigencia de tasa de registro y mantenimiento, carácter jurídico de la contraprestación que se exige (tasa precio público, posibilidad de aplicación del principio de reserva de Ley en materia Tributaria)

---

12 Véase http://www.nic.cl/anuncios/1999-11-24.html

13 Dispone el inciso final del artículo 7° que "Las personas naturales o jurídicas que no residan en Chile podrán solicitar inscripciones de dominios haciéndose representar por alguna persona con domicilio en el país. Este representante actuará como Contacto Administrativo, y se le considerará como el Solicitante para todos los fines de esta Reglamentación, excepto que el dominio será inscrito a nombre del que le haya encomendado esta representación. De esta situación se deberá dejar constancia expresa en la solicitud de inscripción del nombre de dominio."

Como hemos señalado con anterioridad, el NIC-CHILE cobra tasas por otorgar un nombre de dominio, por mantención, por renovación y una consignación por solicitud de revocación.[14]

En la línea que hemos expresado, el DCC realiza deferentes prestaciones de servicios, los cuales hemos descrito precedentemente y por la cual se pagan los impuestos correspondientes. Estamos en el ámbito privado y la contraprestación que se paga en virtud de estas actividades, no tiene carácter público y no es posible aplicarle el principio de reserva tributaria.

3. EXISTENCIA DE CONFLICTOS

a) ¿Consta la existencia de Conflictos?

Sí. En la actualidad el NIC-CHILE contiene en su página web varios enlaces, uno de los cuales señala que nombres de dominio se encuentran en conflicto.

De esta forma al 31 de enero del presente año existen 549 dominios en conflicto.

b) Nº de casos en que se ha dictado resolución judicial o administrativa y breve descripción de los mismos.

En nuestras manos sólo conocemos de tres acciones judiciales que se dicen relación con casos de nombres de dominio. Todos ellos por la vía del recurso de protección, o sea, una acción de carácter constitucional que tiene por objeto restablecer el imperio del derecho y asegurar la debida protección del afectado. Sin embargo, estos recursos no prosperaron por diversas razones que pasaremos a exponer:

- Casos inversiones.cl y desarollodeproyectos.cl

Si bien estos casos son distintos, hemos preferidos referirnos a ellos en conjunto pues ambos fueron rechazados por extemporáneos. En ambos casos se encontraba inscrito con anterioridad el nombre de dominio y se alegaba por las partes recurrentes que se infringía la propiedad industrial. La corte de Apelaciones de Santiago resolvió que el recurso se había interpuesto fuera de plazo y por lo tanto los rechazó por extemporáneo (15 días contados desde la ejecución del acto o la ocurrencia de la omisión o, según la naturaleza de estos, desde que se haya tenido noticias o conocimiento cierto de los mismos).

- Caso Ondac Chile Ltda.

Este es a nuestro juicio el caso más importante sobre el que han resuelto nuestros tribunales debido a que se pronuncia sobre el fondo de la controversia. Es por lo anterior, que haremos un resumen del fallo en los puntos que estimamos más importantes.

Los Hechos:

Con fecha 31 de Junio de 1998 la sociedad ONDAC Chile Ltda. solicita al DCC el registro de la sigla "ondac.cl" como nombre de dominio en Internet en el Registro de Nombres de Dominio cl. Sin embargo, la solicitud se rechazó porque el dominio pedido se encontraba inscrito a nombre de otra empresa "Asesorías, Programas y Textos Computacionales Ltda."

La recurrente expresa que "Asesorías, Programas y Textos Computacionales Ltda." al inscribir la sigla "on-

---

14 Tabla de Tarifas Vigentes: Solicitudes de creación de dominios: $25.000 (IVA incluido) Este pago cubre los dos primeros años de operación del dominio. A este mismo pago están afectos las revalidaciones y las transferencias de dominios. Mantención bi-anual: $10.000 (IVA incluido) Esta tarifa debe pagarse cada vez que se cumplen dos años desde la última vez que se le cobró a ese dominio, y cubre los dos siguientes años de operación. No se cursarán cobros de este tipo antes del 9/9/2000.Examen de Admisibilidad de una Solicitud de Revocación, Monto de la Consignación: 10 UF. http://www.nic.cl/aranceles.txt

dac.cl" ha violado la protección que la ley N° 19.019 otorga al recurrente y que por lo tanto se estaría violando la Garantía constitucional consagrada en el N° 25 del artículo 19 de la Constitución Política de la República y el artículo 20 letra h) de la ley señalada.

La recurrida informó señalando que al practicar la inscripción de la sigla antedicha no tuvieron otra intención que la de ofrecer sus servicios a la sociedad "ondac.cl", sin utilizar dicha inscripción bajo ningún respecto en espera de lograr un acuerdo con dicha sociedad.

Por su parte el NIC-CHILE evacuó el informe correspondiente señalando, en términos generales, que la inscripción en cuestión se había efectuado de acuerdo al reglamento que ellos tenían.

La Corte de Apelaciones señaló en cuanto a la actuación del NIC-CHILE que "su actuación ha sido legal, no discriminatoria y carente de arbitrariedad".

En cuanto a la actuación de la recurrida expresó que "al emplear para su registro la sigla "ondac.cl" como nombre de dominio en Internet en el Registro de Nombres de Dominio CL (NIC CHILE), *puede* haber infringido las normas de la ley N° 19.039, al amparo de la cual la recurrente tiene registrada, como marca comercial, la expresión "ondac", materia que no cabe analizar dentro del ámbito jurisdiccional del recurso de protección, tanto, por ser una materia especial cuyo conocimiento se encuentra dentro de la órbita de competencia de otros órganos, cuanto porque el procedimiento de protección de una marca comercial se encuentra reglado por la referida Ley N° 19.039 sobre propiedad industrial y por su reglamento, el D.S. N° 177, procedimiento que excede al que corresponde aplicar en un recurso de protección."

Por estas razones se rechazó el recurso, pero dejando en claro que existen otras alternativas para solucionar el ataque a una marca comercial.[15]

Por último, es necesario señalar que existen varios casos de conflictos de nombres de dominio en que se ha llegado a acuerdo gracias al procedimiento de arbitraje.[16]

c) Mecanismos para lograr la recuperación de un nombre de dominio.

A nuestro juicio, en nuestro país existen mecanismos emanados del legislador (en sentido amplio) y aquellos que no lo son.

Los primeros son aquellos que están regulados por cuerpos normativos, sean legales o constitucionales. Ejemplo de estos mecanismos lo constituyen el procedimiento establecido en la ley N° 19.039 sobre propiedad industrial y por su reglamento, el D.S. N° 177, como también el mismo recurso de protección consagrado en el artículo 20 de la Constitución Política del Estado que, a nuestro entender, puede ser aceptado en ciertas circunstancias. En este grupo también se incluyen las normas sobre competencia desleal.

En cuanto a los segundos, nos encontramos frente a la reglamentación que ha sido dictada por el NIC-CHILE y que consagra la denominada "acción de revocación" de un nombre de dominio y que puede ser ejercitada dentro del plazo de tres años contados desde la asignación del dominio que se discute.

Esta acción constituye un gran avance y es admitida a tramitación previa consignación en los casos regulados por el reglamento[17].

---

15 Sin embargo, es preciso destacar que la jurisprudencia es vacilante en cuanto a utilizar el recurso de protección para solucionar problemas de marcas, basta recordar el famoso caso de "telefónica" en que el recurso fue acogido.

16 Un ejemplo lo constituye el dominio "presto.cl" que era disputado por SOFT S.A. y D&S. La solución consistió en la creación de un sitio web en que se encontraban dos alternativas sobre las cuales hacer click y que correspondían a las dos empresas señaladas.

17 Es el artículo 20 y siguientes el que regula esta materia al disponer que: "De las Revocaciones de Dominios

Un último comentario con relación a esta acción de revocación y es que si estimamos que entre el solicitante de un nombre de dominio y el DCC existe un contrato de adhesión, la acción de revocación no podría operar con efecto retroactivo porque el reglamento constituye parte de un contrato del cual emanan derechos personales y sobre los cuales se tiene un derecho de propiedad. Por ello, al tratar de aplicar otro reglamento diferente al que existía a la época de la contratación del servicio que asigna un respectivo nombre de dominio, se estaría infringiendo el derecho de propiedad sobre los derechos personales, susceptible de recurrirse vía acción de protección.

Es el artículo 20 y siguientes el que regula esta materia al disponer que: "De las Revocaciones de Dominios

20.- Toda persona natural o jurídica que estime gravemente afectados sus derechos por la asignación de un nombre de dominio podrá solicitar la revocación de esa inscripción, fundamentando su petición según lo dispuesto en el artículo 21 de la presente reglamentación. La acción de revocación descrita en este párrafo, prescribirá dentro del plazo de tres años, contados desde la fecha de asignación del dominio que es objeto de controversia.

21.- Para los efectos de solicitar la revocación de un dominio inscrito ,será necesario que el reclamante:
e. solicite a NIC Chile por escrito, la revocación de dicho dominio, indicando los argumentos en que se funda, y
f. consigne la tarifa correspondiente al examen de admisibilidad, a nombre del árbitro que NIC Chile designe para la realización de dicho examen.
Recibida la solicitud de revocación, NIC Chile designará un árbitro de la nómina del turno, quien efectuará un examen de admisibilidad respecto de la solicitud. Efectuada la consignación para los efectos de este examen, a nombre del árbitro designado, NIC Chile le enviará los antecedentes para su análisis.
Si producto de dicho examen resultare admitida a tramitación la solicitud de revocación, NIC Chile notificará de ésta a las partes involucradas, vía correo electrónico. La tramitación de una solicitud de revocación se sujetará a las reglas del procedimiento de MEDIACIÓN Y ARBITRAJE.
22.- Será causal de revocación de un nombre de dominio el que su inscripción sea abusiva, o que ella haya sido realizada de mala fe.
La inscripción de un nombre de dominio se considerará abusiva cuando se cumplan las tres condiciones siguientes:
a. Que el nombre de dominio sea idéntico o engañosamente similar a una marca de producto o de servicio sobre la que tiene derechos el reclamante, o a un nombre por el cual el reclamante es reconocido.
b. Que el asignatario del nombre de dominio no tenga derechos o intereses legítimos con respecto del nombre de dominio, y
c.Que el nombre de dominio haya sido inscrito y se utilice de mala fe.
La concurrencia de alguna de las siguientes circunstancias, sin que su enunciación sea taxativa, servirá para evidenciar y demostrar la mala fe del asignatario del dominio objetado:
a.Que existan circunstancias que indiquen que se ha inscrito el nombre de dominio con el propósito principal de venderlo, arrendarlo u otra forma de transferir la inscripción del nombre de dominio al reclamante o a su competencia, por un valor excesivo por sobre los costos directos relativos a su inscripción, siendo el reclamante el propietario de la marca registrada del bien o servicio,
b. Que se haya inscrito el nombre de dominio con la intención de impedir al titular de la marca de producto o servicio reflejar la marca en el nombre de dominio correspondiente, siempre que se haya establecido por parte del asignatario del nombre de dominio, esta pauta de conducta.
c. Que se haya inscrito el nombre de dominio con el fin preponderante de perturbar o afectar los negocios de la competencia.
d. Que usando el nombre de dominio, el asignatario de éste, haya intentado atraer con fines de lucro a usuarios de Internet a su sitio web o a cualquier otro lugar en línea, creando confusión con la marca del reclamante.
Sin perjuicio de lo previsto en los párrafos anteriores, la concurrencia de alguna de las siguientes circunstancias, sin que su enunciación sea taxativa, servirá para evidenciar y demostrar que el asignatario del dominio objetado no ha actuado de mala fe:
a. el asignatario del dominio demuestre que lo está utilizando, o haciendo preparaciones para utilizarlo, con la intención auténtica de ofrecer bienes o servicios bajo ese nombre,
b. Que el asignatario del nombre de dominio sea comunmente conocido por ese nombre, aunque no sea titular de una marca registrada con esa denominación, y
c. Que el asignatario esté haciendo un uso legítimo no comercial del dominio ("fair use"), sin intento de obtener una ganancia comercial, ni con el fin de confundir a los consumidores.

Si el resultado del procedimiento de mediación y arbitraje respecto de una solicitud de revocación fuere favorable al reclamante, NIC Chile procederá a transferir el dominio a éste, quien deberá cumplir con los requisitos de asignación, esto es, el pago de la tarifa y el envío de la documentación respectiva, dentro del plazo de 30 días. Si así no lo hiciere, el dominio será eliminado."

Figuras Delictivo-Informáticos tipificadas en Chile

Por Marcelo Huerta Miranda (Chile)
Abogado,
Mag. Iur Unds Soziologie fur Juristen, U. Salzburg,
Presidente de la Asociación de Derecho e Informática de Chile

Con la entrada en vigencia de la ley 19.223, promulgada con fecha 28 de mayo de 1993 y publicada en el Diario Oficial Nº 34.584, de fecha 7 de junio de 1993, se introducen a nuestro ordenamiento jurídico diversas figuras penales relacionadas con los delitos informáticos, los que a continuación pasaremos a analizar.

DESARROLLO Y ANALISIS DE LAS FIGURAS DELICTIVO INFORMATICAS TIPIFICADAS EN LA LEY

I. SABOTAJE INFORMATICO A LOS SISTEMAS DE TRATAMIENTO DE INFORMACION.

I.1. Generalidades

Definición: "Es toda conducta típica, antijurídica y culpable que atenta contra la integridad de un sistema automatizado de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él"[1]

Este delito se encuentra en sus diversas modalidades en los artículos 1º y 3º de la ley 19.223, los que para efectos pedagógicos reproducimos a continuación:

Artículo 1º.- "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Artículo 3º.- "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en su grado medio".

I.2. El sujeto activo en el sabotaje informatico.

En relación al sujeto activo debemos decir que se entiende por tal a quien realiza toda o una parte de la acción descrita por el tipo penal.

Como ya hemos tenido ocasión de ver, el legislador optó por utilizar la expresión "el que", de manera tal de no restringir el tipo penal a la existencia de un sujeto calificado, de acuerdo a tendencia imperante en la actualidad en el derecho comparado, de dotar de una mayor amplitud, flexibilidad y operatividad al delito de sa-

[1] Los Autores.

botaje, con lo cual coincidimos siguiendo especialmente a A.Sneyers y a M. Mörenschlager.

I.3. Sujetos pasivos

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.[2]

En sentido restringido es pues, subjetivo pasivo del delito de sabotaje informático la persona titular del bien jurídico lesionado, sea esta natural o jurídica.

Más en un sentido amplio, atendido el especial bien jurídico que esta normativa introduce a nuestro ordenamiento, creemos que su interés trasciende al conglomerado social e incluso al Estado de Chile, perjudicados al mismo tiempo en su normal funcionamiento por la acción delictiva.

I.4. Elemento objetivo

Para el análisis de las acciones que lo determinan y que la ley tipifica en cada uno de los artículos de la presente ley, distinguiremos entre;

a. Acciones contra el sistema de tratamiento de información.

b. Acciones contra el funcionamiento del sistema de tratamiento de información, y

c. Acciones y conductas que afectan los datos contenidos en un sistema de tratamiento de la información.

ANALISIS DE CADA UNA DE ESTAS ACCIONES Y CONDUCTAS.

a. Acciones contra el sistema de tratamiento de la información.

Esta categoría comprende tanto la destrucción o inutilización de un sistema automatizado de tratamiento de la información, respecto de la totalidad de este, como asimismo, en cuanto a sus partes componentes.

Los acciones de destruir e inutilizar el sistema de tratamiento de la información, constituyen un atentado de tipo directo, por cuanto importan un daño de tipo permanente o irreversible.

a.1. Respecto de la totalidad del sistema de tratamiento de la información.

La conducta punible apunta a deshacer o quitar forma a un sistema de tratamiento de la información sea en su elemento lógico (software) y material (hardware).

Respecto del elemento lógico (software) este, por su naturaleza jurídica, escapa a la esfera de protección penal común, precisando una tutela especial cuando las acciones punibles son realizadas mediante la ejecución de medios de tecnología computacional, con resultado típico destrucción o inutilización.

El elemento material por su parte (hardware), su naturaleza de bien corporal mueble implica que al consumarse su verbo rector en el tipo, deba ser sancionado por la figura del delito de daños del artículo 484 de nuestro Código Penal.

Lo señalado precedentemente respecto de las acciones típicas en calidad de consumadas, en nada obsta a la posibilidad de sancionar de acuerdo al artículo 1º la tentativa si se da en el supuesto lugar al principio de ejecución por medios directos y falten a la sazón, 1 o más para la consecución del fin.

Creemos que también cabrá sancionar estas acciones en calidad de frustradas en la medida que exista una voluntad dolosa por parte del sujeto activo de acción, de cometer el ilícito, el cual no se verifica por causas ajenas a su voluntad.

a.2. Respecto a las partes componentes del sistema de tratamiento de la información.
Las acciones para destruir e inutilizar las partes o componentes de un sistema también alcanzan su protección en el artículo 1º de la ley.

Originalmente, el proyecto de ley sobre el particular sólo se refería a la totalidad del sistema, pero luego, como tuvimos la oportunidad de apreciar en la historia de ley 19.223, su paso por la Comisión de Constitución, Legislación y Reglamento determinó su modificación.

En ella se aprobó la idea de brindar protección legal también a las partes componentes de un sistema de tratamiento de información para evitar el vacío legal que en el primer supuesto se producía para lo cual se optó por legislar en forma amplia.

b. Acciones contra el funcionamiento de un sistema de tratamiento de la información.

Estas, a su vez, admiten la siguiente subclasificación:

b.1.-Impedir el funcionamiento del sistema.

Impedir según el diccionario de la RAE.[3], significa: "estorbar, imposibilitar la ejecución de una cosa". Del latín impedire, implica que no puede usar de sus miembros ni manejarse para andar.

De manera que prolongándonos en esta definición podemos concluir que la conducta típica en este caso no atenta en contra de la existencia misma del sistema de tratamiento de la información, sino que en contra de su desempeño, de su manejo; el cual es el objetivo fundamental de este y para cuya eficiencia fue construido. En este sentido, este sería, por lo tanto, un atentado de carácter indirecto.

Pese a lo anterior, la norma legal en cuestión al ocuparse de sancionar este delito, hace suyo el fundamento de la protección al bien jurídico que esta ley incorpora, (la pureza, calidad e idoneidad de la ciencia informática) y penaliza este atentado de la misma forma que la destrucción del sistema, sin atender a la magnitud, ni la transitoriedad o reversibilidad del daño que se produzca, pues como ya señalamos, no se funda en el patrimonio.

b.2.- *Obstaculizar el funcionamiento del sistema de tratamiento de la información.*

Para el diccionario de la RAE[4], la palabra obstaculizar significa: " Impedir o dificultar la consecución de un propósito".

De suerte que, en cuanto a su acepción y repercusión esta dificultad se traduce en un entorpecimiento en el funcionamiento de un sistema, sin perjudicar la existencia del mismo, por lo que no encontramos inconveniente en hacer suyas las consideraciones señaladas precedentemente y las que damos por reproducidas.

---

3 Diccionario de la Real Academia de la Lengua Española. Tomos I y II. Edit. Espasa-Calpe, 1984.

4 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

b.3.- Modificar el sistema de tratamiento de la información o de sus partes componentes.

De acuerdo a su definición, esta palabra cuya raíz latina modificâre, en su acepción filosófica significa: "Dar un nuevo modo de existir a la substancia material". (De acuerdo al diccionario de la RAE[5]). Nos indica que la expresión fue tomada por el legislador en un sentido amplio, relativo a mutar la esencia o forma de una de una cosa.

La cosa, en este caso el sistema de tratamiento de la información, debe entenderse mutada en razón del objeto o función para la que fue concebida, es decir en razón de su eficiencia.

Un sistema de tratamiento de información está concebido y orientado por su naturaleza a satisfacer determinados requerimientos específicos de un determinado usuario por medio de las ciencia informática, y para el cual es diseñado, motivo por el cual su funcionamiento debe ser idóneo. De manera que se varía su forma de servir se desviará de su objeto específico.

Lo anterior nos lleva a reflexionar sobre el aspecto probatorio de este tipo de atentado, para lo cual pensamos que el juez deberá no sólo apoyarse en la comparación del funcionamiento actual del sistema en relación con su funcionamiento original, sino que además buscar auxilio en las especificaciones de requerimientos u otros documentos que lo ilustren sobre sus características y funcionamiento.

Artículo 1º, inciso 2º :

La figura contenida en el proyecto fue objeto de modificación durante la tramitación de la presente ley, tal cual señalaremos a continuación.

El artículo 1º, inciso segundo, señala el Diputado Viera-Gallo[6] en su moción; que "siguiendo la tendencia de la doctrina contemporánea, establece una causal de agravamiento de la responsabilidad, cuando como el resultado del daño a los programas se produce, además, el de los datos contenidos en el sistema".

Así la figura en el proyecto original era una causal de agravamiento de la responsabilidad en el evento que el daño al sistema de tratamiento de la información se tradujera además en él de los datos contenidos en el mismo.

Luego de la tramitación del proyecto de ley el inciso 2º del artículo 1º, fue modificado, quedando en la actualidad de la siguiente manera:

"Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Respecto de la actual redacción que presenta este inciso 2º, existen dos corrientes de opinión:

a) Para algunos, esta sería una causal de agravamiento de la responsabilidad, en el evento de que, como consecuencia del daño producido al sistema de tratamiento de la información, se dañan los datos contenidos en el sistema.

b) Para otros, la actual redacción del inciso 2º, se refiere más bien al concurso ideal de delitos, situación que como todos sabemos, está resuelta en nuestro Código Penal en su artículo 75, de manera tal que este inciso resulta repetitivo en relación a la norma legal citada.

---

5 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.
6 Ob. Cit. Boletín Oficial Nº 412-07, de la H. C. de Diputados y Senado de Chile.

Por otra parte la vaguedad del término "afectar" utilizado por el legislador, ante la exigencia propia de especificación del derecho penal, contribuiría a fundar los dichos de aquellos que se pronunciaron por estimar que aquí se incurrió en un error de técnica legislativa, razón por la cual su inclusión es desafortunada.

c. Conductas que afectan los datos contenidos en un sistema de tratamiento de la información.

Se encuentran consagradas en el artículo 3º, de la presente ley, que dispone;

Artículo 3º.- "*El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información*, será castigado con presidio menor en su grado medio".

Aquí el elemento objetivo se desarrolla a través de tres tipos de conductas: 1. Alterar, 2. Dañar, o 3. Destruir los datos contenidos en un sistema de tratamiento de información.

Análisis:

La pena asignada al sujeto activo en estas conductas es alta, pero ello se justifica plenamente en este caso *pues la integridad de los datos almacenados en un sistema de tratamiento de información, antes era sólo protegida* penalmente mediante las normas relativas al delito de daños que protege la propiedad corporal.

Con el avance de los conocimientos en estas materias y gracias a una mayor conciencia de la importancia de la información en las sociedades modernas, nuestro mundo, el derecho, ha optado por tomar la iniciativa y crear nuevas figuras penales específicas para amparar la información como objeto intangible, estableciendo un marco normativo de protección a la intimidad.

Vademécum de las posibles conductas objetivas:

1. La alteración de datos:

Alterar según el diccionario de la RAE[7] significa: "Cambiar la esencia o forma de una cosa".

El dato entendido en el anteproyecto de ley como, "todo hecho representado bajo una formula convencional apropiada para su comunicación, interpretación o tratamiento, sea por el hombre o por medios automáticos", *en la medida que es cambiada su forma o su esencia, afectará en definitiva la información, lo que supone* una pérdida de calidad y pureza de técnica informática en relación con los sistemas de tratamiento de la misma, bien jurídico protegido en la ley 19.223.

El dato en el proyecto de ley 19.223, fue tomado en un sentido amplio por el legislador, no limitándolo sólo a los datos personales, con el objeto de dotar a la disposición de flexibilidad y de operacionabilidad.

Inicialmente, el proyecto de ley se refería a la "manipulación de datos", que estaba concebida de manera omnicomprensiva de;

1. La introducción, 2. La transformación, 3. La difusión, y 4. La alteración.

Durante su tramitación, el proyecto de ley fue objeto de indicaciones que determinaron que las conductas de los números 1, 2 y 3 fueran eliminadas del texto legal.

No obstante lo anterior, pensamos que la voz alterar, es omnicomprensiva de conductas como el ingreso de datos erróneos, el borrado de datos verdaderos, de *transformaciones y desfiguraciones de los datos, y en*

[7] Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

general, de toda conducta que implique el cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla.

Estas conductas, como bien se señaló en la historia de la ley, están recepcionadas, aunque con distintas denominaciones y sistematizadas en el derecho comparado.

2. Dañar o destruir los datos:

Dañar, significa "Maltratar o echar a perder una cosa". (Diccionario de la RAE[8]).

En relación con los datos contenidos en un sistema de tratamiento de la información esta se entiende como una conducta destinada a perjudicar la integridad de la información, lo que plantea la noción de un perjuicio, maltrato o afectación de una cosa.

Perjudicada la integridad de un sistema de tratamiento de la información, se afectará el fin u orientación específica del mismo, lo que en el caso de dañarse implica una conducta de carácter transitorio y reversible.

Destruir, de acuerdo a la RAE[9] implica, "Deshacer, arruinar o asolar una cosa...".
En razón de su significado implica un concepto amplio, permanente e irreversible, cuya entidad se traduce en la pérdida de los datos a través de su desfiguración.

I.5. EL ELEMENTO SUBJETIVO.

I.5.1. CONSIDERACIONES.

Como cuestión previa debemos señalar que este elemento del delito informático aparece constituido, en el caso del sabotaje informático, por el dolo que en el caso referido, debemos concluir que se trata del dolo directo.

El estudio fidedigno de la ley cuyas actas hemos tenido a la vista, nos demuestra que para aceptar esta concepción en este tipo de ilícitos hubo de sortear una serie de dificultades, dadas las diferentes posiciones doctrinarias de los legisladores.

Durante la discusión, algunos parlamentarios divergieron de la moción, aduciendo que "si la intención es sancionar a la persona que con intención y propósito realiza la conducta descrita en la ley, a la que lo hace con plena conciencia de la criminalidad de su acción y pese a ello", debería utilizarse la expresión "maliciosamente"

Otros legisladores fueron contrarios a esta opinión, ya que "otros diputados, en cambio, no fueron partidarios de emplear la expresión maliciosamente, por cuanto se exigiría un dolo específico con el cual tipo penal resultaría inaplicable para la mayoría de las situaciones".

La Comisión de Constitución, Legislación y Justicia aprobó por mayoría de votos la exigencia del dolo directo a través de la utilización de la palabra "maliciosamente".

Durante la discusión del proyecto en la Cámara de Diputados volvió a plantearse el tema del dolo en la parte subjetiva del tipo delictivo. Cabe señalar, al efecto, que el Diputado señor Hernán Bosselin expresó que "de incluirse la expresión maliciosamente a estos tipos, en la práctica será muy escasa su aplicación porque "maliciosamente" impone una carga probatoria difícil de acreditar".

---

8 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

9 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

No obstante las divergencias expresadas, el proyecto fue despachado en particular y en general para ser conocido en la Cámara Alta o Senado. En la Comisión de Constitución, Legislación, Justicia y Reglamento donde fue estudiado primitivamente, también se mantuvo la exigencia de un dolo directo.

En el Senado algunos legisladores como el señor Fernández, la señora Feliú y el señor Alessandri plantearon la posibilidad de reconciliar la exigencia del dolo directo, posición que fue desechada en definitiva, aprobándose el proyecto de ley con la referida exigencia.

I.5.2. CONSIDERACIONES SOBRE EL TIPO DE DOLO QUE INTEGRA EL ASPECTO SUBJETIVO

Del delito de sabotaje informático.

El estudio del proyecto legislativo nos lleva a determinar que tipo de dolo consultó el legislador al utilizar el vocablo "maliciosamente" en la descripción del tipo delictivo indicado en el epígrafe.

Esta cuestión nos lleva a delimitar el concepto de dolo que siendo una noción jurídica de tanta importancia no tiene, como es sabido, una definición en nuestra legislación positiva y tampoco ella existe en la doctrina, dada la variedad que ella puede asumir en los diversos tipos de delitos, donde los pareceres se inclinan por darle preferencia al elemento voluntad, teoría de la voluntad, preconizada por Carrara, Almeña, Manzini, Binding, Belin, etc., o en el elemento intelectual, o teoría de la representación, seguida por Franz Von Liszt y Edmundo Mezger.

Para delimitar, en consecuencia, el concepto de dolo debemos tener presente que en nuestro Código Punitivo el artículo 2º ha hecho sinónimas las expresiones "dolo" y "malicia". Igualmente en su artículo 490 se utiliza el vocablo "malicia" para aludir al "dolo". Asimismo observamos que para definir el delito el artículo 1º usa el término "voluntarias" como correspondiente a "dolosas", todo lo cual nos lleva a determinar que en nuestro ordenamiento penal la base de el elemento subjetivo lo constituye la razón y la voluntad.

Ahora bien, la expresión "maliciosamente" que se utiliza en los artículos 109, 161, 196, 198, 204, 221, 224, 256, 338, 342 y 395 se emplea según autorizadas opiniones con el significado de "intencionalmente", o sea, conociendo en forma total la conducta que se lleva a cabo, o más precisamente, procurando que esta se verifique con todos sus efectos propios, lo cual corresponde a una forma de dolo que debe ser calificado como directo.

I.5.3. Clasificaciones del dolo.

Llegados a esta altura de nuestra exposición, estimamos del caso hacer un breve escolio respecto de la clasificación del dolo más conocida en la doctrina y que, por ende, es la que debemos considerar en el caso en estudio.

Digamos entonces que la clasificación más conocida es la que hace un distingo entre dolo directo, el dolo de las consecuencias seguras y el dolo eventual.

-DOLO DIRECTO es la forma más característica de dolo. Se presenta cuando el sujeto activo no sólo realiza la conducta típica de modo voluntario y consciente, sino que está animado del propósito preciso de obtener la producción del hecho jurídicamente reprobable inserto en dicha conducta.

-DOLO DE LAS CONSECUENCIAS SEGURAS o como lo denominaba Jiménez de Asúa "dolo de las consecuencias necesarias" estimándolo una especie de dolo directo. Se presenta en el caso que entre lo previsto y lo deseado por el agente no hay una plena concordancia pero si bien parte de las consecuencias no fue querida por el actor, ella fue aceptada como imprescindible para la producción del resultado efectivamente buscado.

-DOLO EVENTUAL es aquella forma de dolo que surge cuando el sujeto se representa la posibilidad de un resultado que no desea pero cuya producción ratifica en último término. Esta forma, como es sabido, ha sido discutida por nuestra doctrina que tenga cabida en nuestra legislación positiva, ya que existe el criterio de don Gustavo Labatut G. que estima que esta forma de dolo debe asimilarse a la imprudencia temeraria y otros, como Cousiño[10], que expresa que en nuestro Código Penal el concepto general de dolo admite todas las clasificaciones que ha destacado la doctrina, entre ellas el dolo eventual, salvo los casos en que el requerimiento del respectivo tipo admite el dolo, strictu sensu y no el dolo eventual.

Existen otras clasificaciones del dolo que carecen de valor jurídico o se inspiran en nociones ajenas a su verdadero concepto como son las que dicen relación con el dolo de impetu, y dolo premeditado ; dolo inicial, coetáneo o subsiguiente ; dolo genérico o especifico ; dolo determinado o alternativo ; y otras que en virtud de lo antes indicado no cabe analizar por ser inaplicables al tema en estudio.

I.5.4. Conclusión.

Entendemos que dado el uso del término "maliciosamente" utilizado respecto del tipo delictivo que analizamos, debemos llegar a la conclusión de que el dolo exigido en esta conducta antijurídica corresponde al dolo directo propiamente tal y el de las consecuencias seguras o necesarias.

En efecto, en el precepto en estudio se sanciona el resultado típico buscado por el agente (dolo directo) como aquel o aquellos resultados típicos no buscados pero que son imprescindibles para la consecuencia del hecho verdaderamente buscado por el agente.

Dada la fórmula empleada en la disposición en estudio, entendemos que no es aplicable al caso en estudio, el dolo eventual.

II. DELITOS DE ESPIONAJE INFORMATICO.

1. Generalidades.

Definición: " Es toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información".[11]

Para el legislador, como consta en la historia de ley 19.223, este delito consiste en la violación de la reserva o secreto de información de un sistema de tratamiento de la misma.-[12]

En el derecho comparado se ha entendido por espionaje informático, aquel delito que consiste en obtener una información de forma no autorizada, sea por motivo de lucro o de simple curiosidad, hecho que implica espiar y procurarse una comunicación o bien una utilización de un sistema de tratamiento de la información en forma desleal, no autorizada.

Este delito se encuentra en sus diversas modalidades contemplado en los artículos 2º y 4º de la ley 19.223, los que reproducimos a continuación:

Artículo 2º.- "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

---

10 Ob. Cit. COUSIÑO MAC IVER LUIS.

11 Los Autores.

12 Ob. Cit. Boletín Oficial Nº 412-07, de la H. C. de Diputados y Senado de Chile. Sesión 50ª del Senado, 11 de mayo 1993.

Artículo 4º.- "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Como señalamos al inicio del presente acápite este delito, en lo que respecta a la ley en comento, admite la siguiente subclasificación que se desarrollará más adelante:

a) Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información.

b) Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

2. El sujeto activo en el espionaje informático.

Antiguamente se pensaba que la comisión de un delito informático era privilegio de algunas personas, de aquellas que poseían altos conocimientos técnicos, en la actualidad, existe un consenso en el derecho comparado de estimar que cualquier persona que no sea experto en informática puede realizarlos, es más , ni siquiera necesita poseer equipos electrónicos costosos para ello.[13]

En nuestro país, en relación al sujeto activo al cual nos referimos al tratar el delito de sabotaje, debemos señalar que el legislador en la ley 19.223 optó por utilizar la expresión "el que", de manera tal de no restringir el tipo penal a la existencia de un sujeto activo calificado o determinado, y dotar de una mayor amplitud a este delito. Concluimos entonces, que la norma establece como regla general la indeterminación del sujeto activo, y excepcionalmente considera una circunstancia agravante la descrita en el inciso 2º del artículo 4º.

Inciso 2º, artículo 4º: "Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Así, en los delitos de revelación y difusión, esta constituye una agravante que forma parte del tipo y en la que se califica al sujeto activo.

La deslealtad que estas conductas suponen respecto de la reserva y secreto, queda agravada cuando el que maliciosamente realiza estas conductas típicas es el responsable del sistema, supuesto, que justifica desde nuestra perspectiva que la pena se aumente en un grado.

Podemos afirmar de esta forma que en este inciso el sujeto activo es calificado, pero desde la perspectiva de su responsabilidad con el sistema de tratamiento de la información, evento en el cual la figura ve aumentada en un grado la pena, por aplicación de las normas generales del Código Penal.

Esta tendencia es mayoritaria en el derecho comparado. Así por ejemplo, en Gran Bretaña se ha establecido de acuerdo con la Data Protection Act de 1984, la obligación para quien almacene datos personales o confidenciales en sistemas de tratamiento de la información de tomar incluso medidas especiales de seguridad, las que de no cumplirse agravarán su responsabilidad.

3. Sujetos pasivos.

De acuerdo al bien jurídico protegido por esta nueva normativa y, entendiendo que el sujeto pasivo es la persona titular del bien jurídico que el legislador protege, desde la óptica del derecho penal estos sólo pueden ser las personas, sean estas naturales o jurídicas.

---

13 Ob. Cit. SNEYERS ALFREDO.

En la actualidad este delito preocupa especialmente a las empresas, es aquí justamente donde se ha hecho más frecuente y donde se caracteriza por que puede ser muy lucrativo para su autor, lo que lo hace especialmente peligroso y con enormes repercusiones técnicas y económicas para estas. En cuanto al conglomerado social e incluso a los estados y organismos internacionales, estos son también sujeto pasivo y pueden verse seriamente amenazados. Al respecto, célebre es el caso descubierto por el Servicio de Contraespionaje de la RFA. en 1989, en el cual un grupo de jóvenes expertos, pagados por la KGB soviética accedieron a los datos de los sistemas de el Pentágono, la Nasa, del Consorcio Franco-Italiano Thomson, del Centro de Investigaciones Nucleares de Ginebra, de la Agencia Espacial Europea y del Instituto Max Planck de física nuclear en Heildelberg entre otros.

Así, es en el campo del espionaje informático donde queda más al descubierto la precariedad de los sistemas de seguridad, incluso estatales y la vulnerabilidad de los sistemas de tratamiento de la información, de los datos en él contenidos y de la gravedad e importancia a nivel internacional del problema de la creciente criminalidad informática.

4. Elemento objetivo.

Para el análisis de las conductas que el legislador tipifica en los artículos de la presente ley como constitutivas de espionaje, hemos agrupado estas en dos categorías, las que a continuación pasamos a analizar;

a) Delitos de apoderamiento, uso o conocimiento indebido de la información contenida en un sistema automatizado de tratamiento de la información.

La ley trata en su artículo 2º de las diversas conductas a través de las cuales se pueden realizar las acciones típicas. De manera que las conductas típicas se clasifican en:

1.- Interferencia de la información contenida en un sistema de tratamiento de la información.

Interferir: Según el diccionario de la RAE[14] significa, "cruzar, interponer algo en el camino de una cosa, o en una acción. Causar interferencia".

Por su parte, *la interferencia* desde el punto de vista de la física, es la "Acción recíproca de las ondas, ya sea en el agua, ya en la propagación del sonido, del calor o de la luz, etc., de que resulta en ciertas condiciones, aumento, disminución o neutralización del movimiento ondulatorio".

Con fecha 4 de agosto de 1994, el Diputado informante de la Comisión de Constitución, legislación y Justicia, señor Espina[15] expresa: "Este es el caso en que, sin tener derecho para hacerlo, un tercero *interfiere* un sistema de software, o un sistema automatizado de información, con el objeto de apropiarse de información ajena".

Por su parte el Diputado señor Viera-Gallo, autor de la moción que contiene el proyecto de ley señaló en la sesión 33ª de 20 de agosto de 1992 que;"La idea, para que quede bien precisa, es que esta interceptación, *interferencia* o acceso al sistema se haga mediante métodos tecnológicos. No se trata de que una persona, por casualidad, entre a una sala donde hay un computador y lea en la pantalla lo que allí aparece, aunque lo haga con el ánimo de apoderarse de la información, sino que, utilizando métodos tecnológicos modernos, realice algunas de las conductas tipificadas en el artículo 2º"[16].

Concluimos tanto en razón de las consideraciones señaladas precedentemente, como del bien jurídico protegido por esta ley, que la interferencia supone una alteración de la calidad, pureza e idoneidad de la técni-

---

14 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

15 Ob. Cit. Boletín Oficial Nº 412-07, de la H.C. de Diputados y Senado de Chile. Sesión 24ª de la C. Diputados, 04 de agosto 1992.

16 Ob. Cit. Boletín Oficial Nº 412-07, de la H. C.de Diputados y Senado de Chile. Sesión 33ª.

ca de la ciencia informática, mediante la acción recíproca de las ondas de la que resulta un aumento, disminución o neutralización del movimiento ondulatorio original de los impulsos eléctricos, operada utilizando métodos tecnológicos modernos, ya sea con el fin de apoderarse de ella, de usarla o de conocerla.

2.- Intercepción indebida de la información contenida en un sistema de tratamiento de la información.

Interceptar según la RAE[17] significa; "apoderarse de una cosa antes que llegue al lugar o a la persona a quien se destina".

La raíz ontológica *intercipêre* es indicativa de quitar, no de interrumpir como lo es interceptus. De manera que la conducta descrita supone que la información contenida y transmitida en un sistema de tratamiento de la misma no dejará por la intercepción de llegar a su destino o destinatario, pues por su naturaleza de bien incorporal no se ve limitada por el apoderamiento, uso o conocimiento a un sólo poseedor.

Creemos que esta es la correcta interpretación de este verbo rector, puesto que de lo contrario, se caería en el absurdo de que en caso de que se interceptara la información con el fin de apoderarse, usar y conocer de ella, y esta de todas formas llegara a su destino o destinatario, no existiría intercepción y la conducta quedaría impune.

Lo anterior, está basado en el concepto y modalidades unánimemente aceptados en el derecho comparado, para el delito de espionaje y su método comisivo, la intercepción.

Así, como señala el profesor de la U. de Beirut, Ulrich Sieber[18], la radiación y los "campos electrónicos" generados por los terminales de computadores *pueden interceptarse*, también analizarse y grabarse desde distancias de hasta 3.000 pies usando televisores estándares y un equipo de grabación que puede obtenerse razonablemente barato y que puede ser almacenado fácilmente por un auto estacionado en las cercanías del centro informático.

Señala además que esta toma de radiación (intercepción), era una técnica usual de los Servicios Secretos del Bloque del Este". *Documentación para una aproximación al delito informático. "Delincuencia informática", pp 73, Iura 1992.*

Al respecto González Ruz[19], profesor de la U. de Granada, citando a Tiedemann, señala que sólo recientemente se ha sabido que ya desde los años sesentas la R.D.A. adiestraba a sus espías en técnicas informáticas y había concebido un plan específico de espionaje en este campo. Esta revelación tardía supone que la información interceptada llegaba a su destino igualmente.

3.- Acceso indebido a la información contenida en un sistema de tratamiento de la misma.

Acceso: de acuerdo al diccionario de la Real Academia Española[20], acceso es la entrada o paso a un lugar.

Por su parte, el adverbio indebido entrega la idea de ilicitud, injusticia, carencia de equidad, no autorizado.

Estimamos, por lo tanto, que el acceso indebido a la información consiste en las pericias tendientes a introducirse en un sistema de tratamiento de la información, burlando todas las medidas de seguridad y resguardo programadas en su entrada, con el fin de allegarse a la información reservada contenida en el sistema, recabarla y eventualmente utilizarla en beneficio o en perjuicio de terceros.

---

17 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.
18 Ob. Cit. SIEBER ULRICH.
19 Ob. Cit. GONZALEZ RUS JUAN JOSE.
20 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

Desde esta perspectiva, el acceso indebido implica una violación de los passwords del sistema, la cual puede haberse producido de manera premeditada por su autor, o bien, accidentalmente, es decir, la vulneración de las medidas de seguridad no estaban en el ánimo del delincuente, sin embargo, una vez en el sistema, el agente se apodera, conoce o utiliza la información confidencial a que no tenía derecho.

La materia relativa al acceso indebido se relaciona directamente con los delitos de hacking y las modalidades o técnicas de acceso, lo cual ya fue tratado en el capítulo anterior.

Es importante tener presente que la Ley 19.223, en comento, no tipificó el delito de hacking en cuanto acceso indebido. La ley, sólo en su art. 2º, se refiere al acceso a secas. Podría presentarse confusión y estimarse que se trata de cualquier acceso, autorizado o indebido. Sin embargo, al utilizarse, en el mismo artículo, la expresión indebidamente, se entrega cierta certeza de que tal acceso debe ser necesariamente indebido. Por lo demás, así se desprende de las actas de discusión del proyecto.

Debido a que el legislador mantuvo en la atipicidad el delito de hacking, se produce que en Chile es impune la conducta del hacker que por pruebas de carácter intelectual o mera diversión accede indebidamente a los sistemas, transgrediendo las medidas de seguridad.

Asimismo, no constituye delito el acceso indebido realizado por un hacker indirecto, con el objeto de cometer sabotaje de datos.

El hacking sólo se consideró a propósito del espionaje. Sin embargo tampoco es sancionable debido a que el acceso indebido es parte de los elementos objetivos del tipo del art. 2º.

5. Elemento subjetivo del artículo 2º.

Consideraciones.

La motivación del agente comisivo, a la luz del art. 2º, puede ser de tres clases. En efecto, la intención del delincuente será la de apoderarse, usar o conocer, en todo caso, indebidamente, la información contenida en un sistema de tratamiento de la misma.

Pues bien, corresponde precisar que es lo que suponen tales verbos.

A) Apoderarse: según el diccionario de la Real Academia[21], apoderarse significa hacerse uno dueño de alguna cosa, ocuparla, ponerla bajo su poder.

Al respecto, al discutir en el senado el proyecto de ley, sesión 50, el Senador Sr. Otero[22] expresó: "El artículo 2º comienza con la frase: "El que con ánimo de apoderarse indebidamente de la información"... Pero las expresiones "apoderarse indebidamente", en materia informática, significan hacerse para uno, quedando fuera dos elementos que también debieran estar en el tipo, que son "usar y conocer", porque debe castigarse no sólo al que se apodera de la información para hacerse de ella, sino también al que interfiera para conocerla, pues muchas veces conocer la información es suficiente como para caer dentro de los términos del proyecto".

Por tanto, la expresión apoderarse implica que el delincuente recabe la información que considera relevante y actúe comportándose como propietario de la misma, es decir, como si tuviera derecho a ella.

---

21 Ob. Cit. Diccionario de la Real Academia de la Lengua Española.

22 Ob. Cit. Boletín Oficial Nº 412-07, de la H. C.de Diputados y Senado de Chile. Sesión 50ª.

El apoderamiento de la información que se contiene en el sistema no se traduce en usarla ni en lucrar con los datos. Es suficiente el sólo hecho de que la información entre en la esfera personal del transgresor.

B) Usar: consiste en hacer servir una cosa para algo, o bien, disfrutar uno alguna cosa, sea o no dueño de ella.

Se vislumbra con claridad que las precisiones formuladas por el Senador Otero fueron certeras. En efecto, la palabra usar traspasa las fronteras del simple apoderamiento y nos ubica en el terreno de las aplicaciones, en la utilización, es decir, del aprovechamiento.

Sin perjuicio de lo anterior, es bastante improbable que una persona se apodere de las informaciones a que no tenía derecho con el mero ánimo de atesorarlas. La regla casi absoluta será la de usar las cosas que se procuran.

Ahora bien, la Ley no exige ánimo de lucro en el uso, por lo tanto, se trata de utilización lato sensu por lo que el delincuente incurre en la conducta típica al usar la información en cualquier cosa.

C) Conocer: implica averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas.

De cara a la Ley 19.223, conocer informaciones se traduce en un ejercicio intelectual destinado a advertir y saber acerca de distintos datos que se encuentran contenidos en un programa determinado o en un banco de datos.

Es difícil imaginar la acción conocer sin que lo conocido no sea utilizado. Desde este punto de vista parece ser que hubiese bastado con la expresión "usar", ya que nadie puede usar sin haberse apoderado antes de la información, ni sin haberla conocido previamente. Sin embargo se dice que lo que abunda no daña y pareciera que el tipo del artículo 2º de la Ley no se menoscaba con las tres expresiones utilizadas.

Lo que si llama la atención es la conjunción disyuntiva "o" que se utilizó entre las palabras usar y conocer. Tal disyunción implica alternativa entre dos o más cosas, personas o ideas. Por lo tanto es lo uno o lo otro, es blanco o es negro, es apoderarse, es usar o es conocer.

Sea como fuere, las expresiones verbales apoderarse, usar o conocer, van acompañadas del adverbio indebidamente. Por ello, cualquiera que sea el ánimo que desarrolle el delincuente, deberá necesariamente ir empapado de un elemento de ilicitud, de un procedimiento contrario a derecho, de una violación a las prohibiciones. Por ello la palabra indebido entrega connotaciones de antijuridicidad a conceptos que a secas son neutros y no revelan una desviación axiológica. La palabra indebidamente valoriza el precepto y pone a la sociedad a resguardo de personas que sin estar autorizadas, y prevaliéndose de un mal uso de las técnicas informáticas, carentes de ética en la aplicación de sus conocimientos, intentan ingresar a los sistemas en que la información se contiene, generalmente con el fin de usarla en su beneficio. Ellos saben muy bien que en las sociedades modernas la información es un bien de incalculable valor.

Respecto del adverbio indebidamente, es necesario recordar que el proyecto en su versión original establecía que "El que sin derecho intercepte, interfiera o acceda a un sistema...". Tal norma era más precisa y a la vez más amplia, ya que dentro de ella quedaba regulado, además el delito de hacking, toda vez que no hacía referencia específica a motivaciones particulares. De tal suerte tipificaba la figura del acceso indebido a un sistema de tratamiento de los datos, fuere para obtener informaciones, usarlas etc., fuere con el sólo ánimo de realizar, por ejemplo un "joy riding".

b) Delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

Siguiendo con el tratamiento del espionaje informático el cual, como dijimos, se regula por los artículos 2º y 4º de la presente ley, corresponde el estudio de los tipos consagrados en la última de las normas citadas, esto es los delitos de revelación y difusión indebida de datos contenidos en un sistema de tratamiento de la información.

Artículo 4º.- "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

En ambos casos, sea en cuanto a la revelación, sea en cuanto a la difusión, lo que aquí se intenta proteger es la fidelidad en la custodia de informaciones, evitándose la vulneración de la obligación de debida reserva que pesa, no sólo respecto de la persona encargada de la administración de la información y los datos, sino que también sobre cualquier otro trabajador de la entidad que tenga acceso a ello.

Se debe partir de la premisa básica, aunque el artículo no lo dice, que se trata de informaciones privadas, reservadas y secretas.

Al respecto, el profesor español Rodríguez Ramos señala que por secreto se entiende comúnmente la información u opinión conocida sólo por un número reducido de personas, que su tenedor quiere mantener reservada.

En lo relativo al elemento subjetivo del tipo, la revelación y la difusión se realizarán "maliciosamente". Es decir, se consagra la aparición de un dolo específico en el agente que hará necesaria la prueba judicial de la malicia, a diferencia de lo que ocurre en el caso del dolo del art. 1º del Código Penal.

Este tipo de dolo consiste en el conocimiento y la intención positiva de revelar o difundir datos contenidos en un sistema de tratamiento de los mismos, a sabiendas de que ello constituye un ilícito y de que se infringe la obligación de sigilo o reserva.

Sabemos que el bien jurídico protegido por los tipos penales creados al amparo de esta nueva legislación es la pureza o idoneidad de las técnicas de la informática. Por nuestra parte, al definir los delitos informáticos, expresamos que si bien tal era el correcto bien jurídico a proteger no era menos cierto que también, en la comisión de esta clase de ilícitos, se lesionaban, de manera colateral, o si se quiere subsidiaria, otros bienes tutelados por el derecho del tipo clásico. Pues bien, el legislador de la ley 19.223 parece en parte alejarse en el art. 4º del bien jurídico pureza de la técnica y más demuestra acercarse directamente a una protección de la intimidad personal, o bien a tutelar el bien información o, por qué no, la libre y leal competencia.

Lo relativo a la *revelación* de los datos contenidos en los sistemas de tratamiento de la información presupone a lo menos la existencia del derecho para el operador de acceso a la información, con la correlativa obligación de reserva, de suerte que no pueda ésta ser conocida por terceros que carezcan de acceso a ella.

En lo relativo a la *difusión,* este precepto durante su paso por el Senado fue modificado a instancia del Senador, señor Miguel Otero L.[23], que planteó a la Sala modificaciones al artículo 4º que decía: "El que maliciosamente revele o transmita"...

Al respecto el senador manifestó que "Aquí habría que cambiar el vocablo "transmita" por "difunda", porque en el fondo se trata de difundir. El concepto "transmitir" limita y restringe el precepto.

La modificación planteada finalmente fue aprobada por la unanimidad de la Sala.
El proyecto de ley del año 1987 que regulaba la actividad informática, (el cual está agregado como anexo

23 Ob. Cit. Boletín Oficial Nº 412-07, de la H. C.de Diputados y Senado de Chile. Sesión 50ª.

de la presente obra), se refería en su párrafo 4º a la difusión de datos. Por tal razón transcribimos aquí dos de los artículos pertinentes.

Artículo 10º.- Se prohibe la comunicación abusiva de datos personales, entendiéndose por tal, la que resulta de cruzar o de relacionar datos totales o parciales entregados con un objeto diferente.

Artículo 11º.- Los datos personales que se utilicen para fines estadísticos sólo podrán ser difundidos en forma general de modo que no puedan ser atribuidos a personas determinadas.

TIPO AGRAVADO DEL INCISO 2º DEL ART. 4º.

Inciso 2º, artículo 4º: "Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado".

Esta constituye una agravante que forma parte del tipo y en la que se califica al sujeto activo en razón de la deslealtad que estas conductas suponen respecto de la reserva y secreto.

De esta forma se califica al sujeto activo desde la perspectiva de su responsabilidad para con el sistema de tratamiento de la información, y no en relación a una especial o eventual capacitación técnica superior. Por ello, y en razón de lo dicho, la figura ve aumentada en un grado la pena.

Marcelo e. Huerta Miranda.

Abogado, postitulado en Mag. Iur Unds Soziologie fur juristen, con doble distinción por la Universitat Salzburg y Licenciado con distinción en Ciencias Jurídicas y Sociales por la Universidad Las Condes, distinguido con el Premio-Beca de Excelencia Académica. Completa su especialización en Derecho Informático y Sociología Jurídica en Austria, en la Universidad Paris - Lodron de Salzburgo. Autor del Libro "Delitos Informáticos", actualmente termina su segunda obra "Vida Privada y Bancos de Datos". Ha desarrollado su investigación en las principales facultades de derecho y centros de informática en Europa. Autor de múltiples artículos especializados en diversas revistas, ha presentado ponencias tanto a nivel nacional como internacional, especialmente su tesis "Zur Theorie des Informatikrechts, Fragen des Zivil -unds Strafrechts", en el Center For International Legal Studies y en el Aula Magna de la Universidad de Salzburgo (Austria) y en el Instituto de Estudios Superiores de Monterrey (Mexico).

En la actualidad compagina funciones de Abogado en la Contraloría General de la República de Chile, con sus labores de Presidente de la Asociación de Derecho e Informática de Chile, es además miembro de la Computer Law Association y del Colegio de Abogados de Chile, entre otros.

RESUMEN DE LA PONENCIA

Con la dictación en Chile de la Ley N° 19.223, que tipifica figuras penales relativas a la informática, y pese a que dicha ley posee sólo 4 artículos, creemos sinceramente, se abre una página y una vertiente en la moderna dogmática y técnica legislativa para el tratamiento de los delitos informáticos, toda vez que se utilizó, por vez primera, un recurso novedoso y correcto al considerar a la pureza e idoneidad de las técnicas de la informática como el bien jurídico protegido en estos delitos, alejándose con ello de las corrientes del sistema europeo continental y del copyright. Es importante precisar en esta exposición cómo tal valor jurídico se afecta de manera directa cada vez que se cometa un ilícito informático, considerando que al cometerse un delito de la informática se afectan de manera indirecta otros bienes jurídicos tradicionales que no deben perderse de vista.

Creemos que el esfuerzo del legislador en la ley Nº 19.223 no bastó para superar el vacío legal existente, ya que se separó el tratamiento del delito informático de un contexto normativo orgánico, por ello que hemos analizado la actual normativa sólo como una parte de nuestra obra y principalmente de nuestra evolución histórica informática, para aprender de nuestros errores, no sin valorar el esfuerzo y el trabajo en la tarea que actualmente acometen para hacerla operativa ante el derecho.

Los delitos de Hacking en sus diversas manifestaciones

Claudio Líbano Manzur (Chile)
Abogado Profesor
Director - Secretario Ejecutivo
Asociación de Derecho e Informática de Chile (ADI-CHILE)

1. GENERALIDADES.

Previo al análisis de esta especial modalidad comisiva debemos detenernos en dos precisiones de especial pronunciamiento.

En primer término, corresponde precisar que entendemos por delitos informáticos, para lo cual me permitiré citar la definición elaborada en conjunto con mi amigo y colega don Marcelo Huerta y plasmada en nuestra primera obra Delitos Informáticos.

Para ello diremos que *Delitos Informáticos* son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

Estimamos que la definición entregada cumple con el requisito de ser omnicomprensiva de las distintas modalidades delictivas que con motivo de esta obra nos ha tocado conocer y de las distintas motivaciones que ellas tienen. Desde este punto de vista, la definición es de carácter amplio y especialmente operativa en el mundo del derecho. Por otra parte, es flexible y no restrictiva, toda vez que permite adscribirla a todo sistema de técnica legislativa que pretenda utilizarse, sea en la realidad nacional o en la experiencia extranjera como más adelante, y por primera vez, se entregará a la comunidad nacional interesada. Por otro lado, la definición es consecuente con nuestros postulados de internacionalización del derecho informático, así como con el necesario uso de una terminología clara y precisa sobre los conceptos técnicos y jurídicos que abraza.

En segundo término, y a grosso modo, me parece pertinente entregar nuestra propia clasificación de los delitos informáticos. Así proponemos proponemos la siguiente clasificación, a la luz del derecho comparado:

1. La manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información. El fraude informático.

Tal manipulación puede realizarse en la entrada de datos al sistema (input), en los programas, en la salida de datos del sistema (output), y siguiendo a Romeo, en el caso de manipulaciones a distancia, mediante la conexión telemática vía módem a un computador.

Esta primera clasificación es de carácter general y envolvente, pues, por regla casi absoluta, todo delito informático se cometerá a través de una manipulación en cualquiera de las fases mencionadas.

2. Delitos de espionaje informático.

Se incluyen las formas de acceso no autorizado a un sistema de tratamiento de la información.

3. Delitos de sabotaje informático.

Incluyen las formas de destrucción y alteración de datos, así como los programas virus.

4. .Delitos de piratería de programas.

Sólo en cuanto se traduzca en la copia indebida de programas por medios informáticos.

5. Delitos de hacking, en sus distintas manifestaciones que se analizarán más adelante.

Luego de estas prístinas distinciones, nos encontramos en condiciones de abordar el quizás el más fulgurante de los delitos informáticos. Para ello es menester formular ciertas precisiones aclaratorias.

El delito de hacking, por constituir fundamentalmente un acceso indebido o no autorizado, induce a la creencia, no errada por cierto, de que este ilícito se presentará como medio o herramienta de comisión de otros delitos informáticos ya tratados, y que, por lo tanto, su característica podría ser la de configurarse como un hecho delictivo necesario para la comisión de otros.

Tal hipótesis en cierta medida es verdadera y comprobable. En efecto, gran parte de las veces los daños o deterioros sufridos por un programa, el espionaje de datos, los fraudes informáticos o la piratería de software, se realizarán a través de un acceso indebido o contra derecho en los sistemas. En tal caso, estimamos que el acceso indebido, léase hacking, sería un delito que se perpetra como medio necesario para la comisión de un ilícito diverso, situación en que, para los efectos sancionatorios y de penalización, se aplicarían las normas generales del derecho penal que rigen el llamado concurso ideal de delitos.

Sin embargo, es legítimo preguntarse acerca de la originalidad e independencia criminológica y típica del delito de hacking, o de otra forma, sobre la posibilidad de que un delito como el que tratamos surja y se consume de manera no asociada o vinculada con los otros delitos informáticos.

Previo a responder directamente esta interrogante, es preciso deternernos a razonar sobre el problema de las motivaciones que entran en juego en la mente del delincuente y que lo inducen a cometer delito.

Es indudable que muchas veces el HACKER (persona que comete el delito de hacking) utiliza el acceso indebido a un sistema de tratamiento de la información con el fin de cometer un fraude informático, un espionaje de datos, piratería o sabotaje en sus distintas manifestaciones. En estos casos el ánimo del delincuente será cometer estos delitos y la violación a la prohibición de acceso no será más que un medio de consumación. Ante esta primera situación motivacional es necesario precisar que para que exista hacking, éste debe estar tipificado de alguna forma en una ley. Por ello, pueden presentarse algunas situaciones que es necesario revisar. En primer término, es posible que el delincuente, al acceder indebidamente a un sistema para cometer, por ejemplo, sabotaje informático, se enfrente a un tipo penal que sanciona el sabotaje y que incluye como elemento del delito el acceso indebido. En este caso, no será posible hablar de delito de hacking ya que el acceso contra derecho era parte integrante del tipo sabotaje. Puede también suceder que la disposición que tipifica el sabotaje informático no considere el acceso indebido como uno de sus elementos objetivos, situación muy probable por cierto en atención a que muchas veces los delitos se cometen por operadores que cuentan con una autorización que les franquea el ingreso a los sistemas, y en tal caso podría considerarse la posibilidad de aplicar un concurso de delitos de sabotaje y hacking en el evento que otra disposición legal regulara separadamente el acceso indebido como delito. Si tal norma no existe, se deberá sancionar exclusivamente el sabotaje.

Un segundo supuesto motivacional del hacker estará determinado por un ánimo que podríamos llamar "no dañoso". En efecto, es posible, y así ha ocurrido muchas veces, que el delincuente busque la violación de la negativa al acceso, entiéndase códigos, passwords, etc., como una forma de autoratificación de sus capacidades técnicas e intelectuales. El hacker perseguirá la satisfacción de lograr vencer un obstáculo y de demostrar que los programadores que dispusieron las medidas de seguridad no pudieron contra su inteligencia. Asimismo, dentro de esta motivación "no dañosa", se encuentran los hackers que buscan burlar los códigos de acceso con la finalidad

del simple divertimiento o por razones de curiosidad. Estas conductas, a pesar de no causar un daño directo y tangible, son delitos en si mismas y deben, necesariamente, estar reguladas y sancionadas.

Luego de estas breves consideraciones, es factible pasar al estudio del delito de hacking, sus modalidades, y la casuística que entregan los autores de las doctrinas comparadas.

2. CLASIFICACIONES DEL HACKING.

De acuerdo a lo expuesto, podemos decir que el delito de hacking admite ser clasificado en dos grandes grupos:

A. Hacking propiamente dicho o Hacking directo.

El hacking propiamente dicho, es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.

La voluntad de divertirse generalmente se traduce en paseos por el sistema haciendo alarde de la intromisión. Es lo que se ha llamado JOY RIDING, o paseos de diversión.

Características de esta clase de hacking.

a. El hacker es una persona experta en materias informáticas, y generalmente sus edades fluctuarán entre los 15 y los 25 años. Es por ello que esta delincuencia se ha nominado "SHORT PANTS CRIMES", es decir, crímenes en pantalones cortos.

b. Su motivación no es la de causar un daño, sino que se trata de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos. Por ello, el hacker siempre buscará notoriedad pública desde el anonimato. Asimismo, perseguirá objetivos cada vez más difíciles de vencer, y elegirá sus víctimas entre empresas y organismos de trascendencia nacional e incluso internacional.

c. Esta clase de hacking no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.

d. Desde un punto de vista estrictamente jurídico, estimamos que se trata de un delito de resultado que se consuma al momento de ser descifrados los códigos de acceso secretos, aún cuando los usuarios no tomen conocimiento del hecho.

Sobre la modalidad del hacking propiamente dicho, el economista español Alfredo Sneyers, en su libro "Fraude y Otros Delitos Informáticos", entrega un caso digno de análisis ocurrido en Inglaterra.

"Dos hackers, Steve Gold y Robert Schifreen, encontraron una brecha en el sistema de seguridad del sistema Prestel de la British Telecom. En octubre de 1985, tuvieron acceso a varias cuentas confidenciales y uno de ellos, Schifreen, pudo introducirse en la casilla de correo electrónico del duque de Edimburgo. Schifreen logró tener acceso no autorizado al sistema Prestel porque empleados de la British Telecom habían dejado las

contraseñas privilegiadas del sistema Prestel en las páginas electrónicas principales del sistema de prueba. Gold y Schifreen informaron a Prestel acerca de esta anomalía y Prestel la corrigió.

Ambos hackers fueron detenidos y, a finales de 1986, fueron juzgados culpables de falsificación y condenados a pagar multas por un total de 1.350 libras (unas 300.000 pesetas) y costas del juicio por unas 1.000 libras (unas 200.000 pesetas)".

Sin embargo, el Tribunal de Apelaciones, al revisar el fallo, estimó pronunciarse por la absolución de los condenados. Textualmente el presidente de aquel alto Tribunal sostuvo: "Su conducta fue la de ganar acceso deshonesto al banco de datos de Prestel mediante un ardid. Esto no constituye una ofensa criminal. Si se desea considerarlo así, es una cuestión de la legislatura más que de los tribunales".

Esta sentencia conduce a que podamos formular ciertas precisiones.

En primer término, el fallo recurrido condenó a los Sres. Gold y Schifreen en calidad de autores del delito de falsificación. Lo que ocurrió, es que ante la ausencia de ley que regulara la actividad de los accesos indebidos, el Juez se vio en la necesidad de recurrir al tipo que pensó más podía asemejarse a las conductas expuestas. La verdad es que debió forzar las características incriminatorias del delito de falsificación, de manera de propiciar el encuadramiento necesario para condenar.

En segundo lugar, el Tribunal de Apelaciones fue más sensato y justo. Consideró que las conductas de los acusados no constituían delito, sin perjuicio de que merecieran un juicio de reprochabilidad. Menciona asimismo que el problema es de la legislatura y en eso tiene la razón. La tipicidad es de competencia de los legisladores, los cuales deben recoger las necesidades sociales de tutela jurídica frente a ciertos hechos no regulados como delitos.

De acuerdo a Sneyers, el Computer Fraud & Security Bulletin criticó la sentencia del Tribunal de Apelaciones expresando que de esta forma el hacking sólo sería sancionado cuando el hacker, a través del acceso indebido cometa fraude u otros delitos, tratando de significar que debe sancionarse el hacking propiamente dicho. Es cierto lo manifestado por tan prestigiosa revista, sin embargo no comprenden que en el caso de Inglaterra el problema pasaba por la ausencia de Ley.

Sin perjuicio de nuestra posición, se han levantado voces expresando que el hacking propiamente tal no es una conducta que pueda ser considerada como delictiva. Se fundan en que tal clase de hacking no constituye ofensa alguna y que castigar al hacker por el simple hecho de acceder significaría pisotear el derecho a la intimidad del hacker. Lo dicho no resiste mayores comentarios si se piensa solamente en que el hacker viola la intimidad de sus víctimas al acceder sin derecho a los programas ajenos.

Al respecto, Ulrich Sieber, se pronuncia en favor de la atipicidad del hacking propiamente dicho, en el caso de que luego del acceso, el hacker de noticia a las víctimas de la manera en que ingresó.

Creemos que tal posición no es sustentable jurídicamente, toda vez que la sóla situación de revelar la técnica comisiva no exime al hacker de la mala utilización que realiza de las técnicas informáticas, las cuales deben ser puras e idóneas de acuerdo a la tendencia chilena que nosotros compartimos. Por otro lado, si nos basamos en los bienes jurídicos múltiples que intentan proteger en el derecho comparado con los delitos informáticos, concluiremos que el hacker que no causa daños o fraudes, si viola la privacidad de los datos, afectando la intimidad entrando, de manera no autorizada, en la propiedad ajena.

Ahora bien, es evidente que la penalización de esta clase de hacking no debe ser de gran magnitud, precisamente atendiendo a que no causa mayores daños y a que el ánimo involucrado no es extremadamente riesgoso. La circunstancia de que el hechor revele a sus víctimas el modus operandi en la violación de la prohibición de acceso, puede ser vista desde dos ángulos: por una parte existe la posibilidad de que el ánimo del hacker sea efectivamente poner a resguardo a las víctimas de nuevas intromisiones; por otro lado, es posible

que el agente delictivo sólo busque vanagloriarse y hacer aún más sarcástica su burla. Sea como fuere, el acceso indebido se produjo y el delito se consumó.

A modo de corolario del presente acápite, citaremos las palabras del experto Sneyers :

"La sociedad debe tomar conciencia de que el hacker es una persona que comete un acto ilegal con pleno conocimiento de causa sólo por el mero hecho de introducirse, sin autorización, en un sistema informático ajeno, exista o no intención de causar un daño o ánimo de lucro".

B. Hacking como medio de Comisión de otros Delitos o Hacking indirecto.

Como se ha dicho, es usual que el hacking, en cuanto acceso indebido, se realice como medio para la comisión de otros delitos como fraude, sabotaje, piratería, y espionaje.

Es usual que los delincuentes informáticos se valgan de accesos indebidos a los programas para cometer ahí sus fechorías.

Los delitos de fraude, sabotaje, etc., pueden cometerse, en general, por dos tipos de personas: en primer término, por aquellos que tienen autorizado el acceso al sistema y que, por ende, conocen, legítimamente, los códigos de seguridad. Se tratará generalmente de trabajadores del área informática de bancos, empresas u organismos del estado. En estas personas se ha depositado un nivel de confianza importante. En segundo lugar, están aquellos que tienen el acceso prohibido o cerrado y que ingresan al sistema a través del desciframiento malicioso del password. Es en este último caso donde el agente comete hacking indirecto.

Como se dijo, lo que determina si el hacking es propiamente dicho o medio de comisión de otros ilícitos es el ánimo o motivación que induce a la comisión del delito. En el caso del hacking que tratamos, el ánimo del delincuente está determinado por su intención de dañar, de defraudar, de espiar, etc. Es por ello que en el hacking indirecto el acceso indebido cede su rol protagónico frente al delito "principal" que se busca cometer.

Tal situación no implica que el acceso indebido como delito desaparece. Sin embargo, para que esta materia quede absolutamente clara, es necesario plantearse algunas hipótesis legislativas.

Un primer supuesto estará determinado por la posibilidad de que una ley sobre la actividad informática, o bien la que introduzca modificaciones relativas a estas materias en los códigos penales, contemple, de manera expresa, en una norma independiente de aquellas que tipifican el fraude, el espionaje, el sabotaje, etc., el acceso indebido o hacking en sus dos clases, como una forma delictiva aislada, es decir, un delito per se.

La segunda posibilidad radica en el supuesto de que la ley incluya el acceso indebido como elemento del tipo fraude, sabotaje, piratería, etc. Por ejemplo, "El que a través de un acceso indebido al sistema de tratamiento de los datos destruya, modifique o altere el contenido de programas o ficheros...". En este caso, no será correcto hablar de hacking como delito independiente, toda vez que el acceso indebido pasa a ser uno más de los elementos objetivos del tipo. Dentro de esta segunda hipótesis, cabe también la posibilidad de que el legislador, en atención a las especiales características de ciertos tipos delictivo informáticos, incluya el elemento acceso indebido sólo en algunas de las figuras y no en todas, y al mismo tiempo exista una norma general e independiente que sancione el hacking en sus modalidades.

La tercera situación es la que se relaciona con la atipicidad del hacking. Es decir, el acceso indebido, cualquiera sea la motivación que presente, no estará sancionado. Esta es, sin duda, la más peligrosa de las alternativas.

Sostenemos que la mejor forma de regular el hacking, en general, es su tipificación en una norma independiente. De esta manera se evitan confusiones y se hace más exiguo el campo de los intérpretes. Por lo tanto el

acceso no autorizado será siempre un delito cualquiera sea el ánimo con que se cometa, sin perjuicio de que tal motivación deba ser un elemento a considerar al graduar la pena aplicable. De esta forma, se salva el problema de los delitos cometidos por personas autorizadas a ingresar a un sistema determinado, los cuales sólo serán sancionados por el delito que cometieron, sin perjuicio de que pueda constituirse una circunstancia agravante de la responsabilidad criminal por el eventual abuso de confianza empleado en la comisión del ilícito.

Así, en el caso de que una persona cometa sabotaje ingresando ilícitamente al sistema, se le sancionará por el concurso delictivo ideal que se produce en el hecho, debido a ser el acceso indebido el medio necesario para cometer otro delito.

Siempre resulta interesante citar un caso. Para ello citaremos a Alfredo Sneyers, quien, de acuerdo a la revista Computer Fraud & Security Bulletin, narra la siguiente hazaña delictual.

"Hoxie, un programador de 24 años de edad, de Houston, Texas, de buena posición económica, fue acusado de robo y arrestado. Negó toda responsabilidad y fue puesto en libertad bajo fianza de 30.000 dólares.

Los hechos:

Según el fiscal, Robert J. Hoxie accedió sin autorización a una base de datos de Greater Houston Credit Bureau de la que extrajo las historias personales completas de cierto número de presidentes de bancos, altos ejecutivos de compañías de petróleo y otros prominentes hombres de negocios. Obtuvo así los números de sus cuentas bancarias y de sus saldos y, lo que es muy importante, información sobre las tarjetas de crédito que tenían.

Se alegó que hoxie solicitó las tarjetas de crédito Master Card y Visa en nombre de sus víctimas; el First City Bank de Dallas las concedió y envió a sus direcciones, en el área de Houston, que figuraban en las solicitudes.

Hoxie reunió un total de 76 tarjetas de crédito en las direcciones que había dado y, disfrazado para no ser reconocido, las utilizó para efectuar retiros de fondos en cajeros automáticos por un importe total de 100.000 dólares.

El fraude duró desde Julio hasta Octubre de 1984, fecha en que un empleado del First City Bank examinó la lista de las "tarjetas delincuentes" y vio el nombre de uno de sus colegas del banco. Habló con él y, naturalmente, éste no sabía nada de la tarjeta concedida a su nombre.

El banco, entonces, examinó todas las tarjetas de crédito en las que los nombres no correspondían a las verdaderas direcciones de sus poseedores y se descubrió que las pérdidas ascendían a un importe total de 100.000 dólares.

Hasta la fecha de la publicación, los investigadores no habían podido establecer aún cómo se había realizado este hacking. Por la evidencia disponible, parece que alguien pudo acceder a la contraseña del jefe de los sistemas, ya que datos tan detallados como los obtenidos por Hoxie no podían haber estado a disposición de los suscriptores normales del Greater Credit Bureau".

Por último, parece ser que el hacking comenzó como un hacking de desafío intelectual o de divertimiento. Con el paso de los años esta modalidad delictiva ha ido pasando a un segundo plano frente al impulso que ha adquirido el hacking delincuencial o indirecto.

3. Técnicas utilizadas por los Hackers para acceder a los sistemas.

Todo hacker, para acceder de manera indebida a un sistema de tratamiento de datos, requiere necesaria-

UNIVERSIDAD
BIBLIOTECA
DE LIMA

mente prevalerse, al menos, de un computador personal, un módem, el número de teléfono de conexión al sistema, el código personal de un usuario autorizado al acceso o el código de apertura de la sesión de trabajo, LOGON, y el password propiamente tal.

Para lograr estos objetivos, se utiliza habitualmente el procedimiento llamado *SCANNING*, que consiste en programar el computador para que realice una gran cantidad de llamados telefónicos en serie con el fin de descubrir el número del sistema de tratamiento al cual se quiere acceder, o bien se utiliza de manera aleatoria hasta descubrir cualquier número telefónico que sirva a los intereses del hacker. Asociado a ello, y con el fin de evitar figurar en los registros computacionales de las compañías de teléfonos y salvar el costo de las llamadas, los hackers intervienen los sistemas de las telefónicas borrando sus registros, o bien cargando el costo de las llamadas a otros usuarios.

Frente a este sistema, Camacho propone como medida de seguridad la utilización del Call Back o de devolución de llamadas. Expresa el jurista, "La eficacia de este dispositivo se basa en que cuando un usuario conecta con el sistema y se identifica válidamente, queda registrada su identificación y a continuación, antes de comenzar la sesión de trabajo, el sistema le desconecta la comunicación e investiga en una tabla asociada a los identificativos de usuarios cual es el número de teléfono real que corresponde a ese usuario, desencadenando una llamada automáticamente del ordenador central al número real del usuario que ha sido identificado, con lo cual se evita que una identificación válida realizada desde un punto no autorizado pueda llegar a penetrar al sistema".

Sneyers, además, indica otros procedimientos destinados a idéntico objeto. Así menciona el llamado *SHOULDER SURFING*, que consiste en espiar directamente a los operadores y anotar el password a través de la observación visual del momento en que el usuario digita la contraseña en el teclado del computador.

Se refiere también a la modalidad *DUMPSTER DIVING*, a través de la cual los hackers pretenden encontrar información relevante y servicial a sus oscuros propósitos en los basureros de los lugares en que funcionan los centros de procesos de datos.

Otro procedimiento mencionado por Sneyers es el denominado *SPOOFING*, por el cual el hacker, falseando su identidad, concerta entrevistas con personeros especializados de los centros de procesamiento. Todo ello con el fin de obtener informaciones que permitan el acceso a los sistemas sin ser descubierto.

Es importante esclarecer que normalmente los hackers no actúan solos. Se mueven dentro de verdaderas mafias en las que comparten informaciones, trafican datos relevantes y cuentan sus experiencias con ánimo pedagógico. Sin embargo, han ido incluso más lejos. Se ha descubierto la operación de grupos organizados de hackers como lo es el CCC, Chaos Computer Club de Hamburgo Alemania. Dentro de las hazañas más espectaculares de estos hackers se cuenta su acceso a los sistemas de la NASA vía red SPAN.

Otro grupo identificado es el MILWAUKEE 414 GANG. Compuesto por jóvenes entre 17 y 25 años, lograron en 1983 ingresar a un sinnúmero de sistemas tanto de los gobiernos de E.E.U.U. y Canadá, así como otros importantes organismos privados y públicos, incluidos los sistemas de la Fuerza Aérea norteamericana en su base de McClellan en Sacramento y de la administración telefónica en Noruega.

Por último, sólo me resta despedirme de esta audiencia, agradeciendo su invitación y las atenciones dispensadas. Hacemos los votos para que el fruto de los debates y de las opiniones aquí vertidas se cristalicen en obras y constituyan verdaderos aportes a la doctrina internacional en general, y para nuestros queridos países en particular.

Es cuanto puedo expresar.

Muchas Gracias.

RESUMEN

El Dr. Líbano es Abogado, especialista en derecho de las tecnologías y de los negocios, titulado con amplias distinciones por la Universidad Las Condes de Santiago de Chile. Asimismo, es pos-titulado en Derecho del Desarrollo del Personal por Carnegie. De otra parte, es asesor legal de los Directorios de distintas empresas multinacionales del área minera y tecnológica. Asimismo, es autor de la Obra Delitos Informáticos por la casa Editorial Conos-Sur. Por otro lado, se encuentra preparando su segunda obra relativa a Regulación Jurídica de las Bases de Datos. Además, es miembro colaborador de la Computer Law Association, y Director, Secretario Ejecutivo de la Asociación de Derecho e Informática de Chile, ADI-Chile.

SUMARIO DE LA PONENCIA

A través de esta ponencia, el autor pretende, previa revisión breve de conceptos básicos, interiorizar al auditor respecto de algunas particularidades del delito informático de hacking, en sus diversas manifestaciones.

Comienza por describir y analizar su propia definición de delitos informáticos, para luego entrar derechamente a formular su original clasificación de los mismos. Luego de ello, pasa a desarrollar distintos aspectos relacionados con la particular forma comisiva denominada Hacking. Bajo esta luz, indaga en las distintas modalidades comisivas, estructura del delito, efectos del mismo y ejemplos y casos prácticos que ilustran las posturas jurisdiccionales frente a esta manifestación punible.

Finalmente, nos señala distintas formas a las que acuden habitualmente los sujetos activos para cometer esta clase de fechorías.

¿Nombres de dominio, marcas o no?"

Dra. Esc. Beatriz Rodríguez Acosta. (Uruguay)
Coordinadora Alterna de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay, Miembro del Centro de Informática Aplicada a Derecho de la Facultad de Derecho (CINADE), A/S Walter González Barone, Procurador, Miembro del Centro de Informática Aplicada a Derecho de la Facultad de Derecho (CINADE).

I. INTRODUCCION

Dentro de esa gran autopista de la información, que es Internet, podemos comprobar que el mundo avanza hacia todas las direcciones, sin detenerse, asimismo vemos como los medios de comunicación han evolucionado uniendo a la casi totalidad del planeta.

Si bien se han producidos cambios favorables, existen otras áreas dentro de Internet, que están dando un tanto que hablar en estos últimos tiempos, y que todavía no se ha llegado a encontrar la solución, como es el caso concreto de la "colisión" existente entre una Marca y un Nombre de Dominio.

Debido a lo expuesto anteriormente trataremos de dar una pequeña síntesis de lo que ha estado sucediendo, a ese respecto, a nivel mundial y lo que sucede en nuestro país, Uruguay.

Como es sabido, por la mayoría de nosotros, se han suscitado dentro de Estados Unidos, dentro de Europa, diversas controversias con respecto a los Nombres de Dominio.

Este es un tema que no está regulado, ustedes dirán en Internet existe una ausencia de regulación, aunque hay en algunas materias un querer de regulación, por lo que en realidad Internet no es un espacio en que el Derecho no encuentre cabida, todo lo contrario. Por esta razón es que la regulación de los Nombres de Dominio es tratada con suma importancia en los diversos congresos y reuniones, la Organización Mundial de la Propiedad Intelectual está tratando de armonizar los criterios en materia de Marcas y Nombres de Dominio, lo mismo sucede en los diferentes países , en especial en el Uruguay.

II. PROPIEDAD INTELECTUAL

Dentro de la doctrina nacional tenemos la definición que nos proporciona el Dr. Siegbert Rippe en su obra A La Propiedad Industrial en el Uruguay @, en la cual Propiedad Intelectual es: **un uso exclusivo, monopólico, excluyente, de los bienes sobre los que recae... derechos que no son estrictamente en la cosa o contra la cosa, ni un crédito contra determinada persona y que además resultan de una concesión que otorga la Administración y cuya duración es temporal.**

Las teorías más antiguas sobre Derechos de la Propiedad Intelectual nacieron en el siglo XVII (época en la cual nadie se imaginaba el avance de los medios de comunicación en qué terminarían) en relación con el voto de pobreza religiosa, siendo en España la Escuela de Salamanca con Francisco Suárez y otros los que se encargaron de su estudio por primera vez.

De acuerdo con las Disposiciones Generales y Principios Básicos del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, incluido el comercio de mercancías falsificadas (ADPICS o TRIPs), art.1: **el Derecho de Propiedad Intelectual abarca todas las categorías de propiedad intelectual que son objeto de las secciones 1 a 7 de la parte II del mismo que son: Derecho de Autor y Derechos Conexos, Marcas de Fábrica o de Comercio, Indicaciones Geográficas, Dibujos y Modelos Intelectuales, Patentes, Esquemas de Trazado (topografía) de los Circuitos Integrados y Protección de la Información no Divulgada.**

II. 1. Marcas

Como en todo concepto vamos a tener más de una acepción de lo qué es la marca, así tenemos:

Breuer Moreno: es el signo con que el industrial, comerciante o agricultor distingue los productos de la industria, comercio o explotación agrícola (Pedro Breuer Moreno, Trat. De Marcas de Fábrica y Comercio, 2da edición, Editorial Robis, Bs. As.,1946, pág.31).

Jorge Otamendi: es el signo que distingue un producto de otro o un servicio de otro (Jorge Otamendi, Derecho de Marcas, Abeledo-Perrot, Bs.As. 1989, pág.7)

Siegbert Rippe: : signo que sirve para diferenciar los productos o los servicios de una empresa de las otras empresas (La Propiedad Industrial en el Uruguay. FCU, 1era. Ed. 1992, pag.37)

Jorge Buslón: ex asesor de la Dirección Nacional de la Propiedad Industrial: es un signo visible que permite distinguir los bienes o servicios de una empresa de los bienes o servicios de otras empresas (las Marcas y la Defensa del Consumidor, en Derecho del Consumidor, FCU, Colección JVS No.34, 1988, pág.79)

La ley 9956 no definía a la marca, pero un antecedente de esta del 11/7/09, sin número, en su art. 1 establece que: cualquier otro signo con que se quiera distinguir los artefactos de una fábrica, los objetos de un comercio o los productos de las industrias agrícola, extractiva, forestal y ganadera es una marca.

Así tenemos que es cualquier signo con que se quiera distinguir bienes o servicios de una empresa de los de otra empresa, siempre que ese signo no sea contrario a la ley.

Actualmente la ley 17011 del 25/9/98 establece en su art. 1 que marca es todo signo con aptitud para distinguir los productos o servicios de una persona física o jurídica de los de otra.

Como vemos la marca es un signo identificatorio que su mal uso o su uso indebido puede llegar a confundir al consumidor, causando un perjuicio a su titular.

II. 2. Nombres de dominio

Dentro de este nuevo mundo se hace necesario poder reconocer o individualizar, dentro de la Red, las diferentes máquinas que en ella están conectadas, para poder identificarlas, recibir y transmitir la información a través de ellas, es que necesitamos el llamado Nombre de Dominio, o Domain Name

Este Nombre de Dominio está dentro de un sistema o DNS, como se lo conoce comúnmente , que consiste en una base de datos que relaciona los nombres con direcciones IP, las cuales si nos ponemos a pensar son las verdaderas direcciones de las máquinas, el que fue desarrollado por el Departamento de Defensa del Gobierno de Estados Unidos, a través de privados. Para que este sistema funcione todos deberíamos utilizar la misma base de datos que interconecte las direcciones IP con los Nombres de Dominio. En suma, los nombres de dominio son: **la localización del sitio de Internet en el cyberespacio,** sería como su domicilio. La misma está dada por una combinación de números convertibles en letras, que generalmente son marcas que identifican a las empresas e instituciones, tratando así que las personas no se vean en la necesidad de trabajar con números y la posibilidad de utilizar caracteres más memorizables.

La finalidad del DNS es permitir el escalado de los nombres de dominio, por medio de una distribución jerárquica de los mismos, de forma que en cada nivel, el dominio delegado es el responsable de asignar nombres unívocos para que no existan duplicidades.

Los primeros tribunales que se han enfrentado a problemas de Propiedad Intelectual emergentes del uso de Internet han sido los de Estados Unidos, ya que se han dado controversias entre marcas famosas por parte

de terceros que las han registrado indebidamente como nombres de dominio. Surgiendo problemas de competencia debido a la falta de límites en esta autopista, poniendo en tela de juicio el principio de la territorialidad.

III. TRATAMIENTO DE LOS NOMBRES DE DOMINIO DE ACUERDO A LA ORGANIZACION MUNDIAL DE LA PROPIEDAD INTELECTUAL.

Dentro de la Organización Mundial de la Propiedad Intelectual el tema de los Nombres de Dominio ha tenido una evolución, ya que estos han adquirido mayor importancia en tanto indicadores comerciales y han provocado conflictos con el sistema de identificadores comerciales que existían ante de la llegada de Internet y que está protegido por derechos de propiedad intelectual.

La OMPI ha emprendido desde 1998, un amplio proceso internacional de consultas. Este consiste en formular recomendaciones a la entidad creada para administrar el sistema de los nombres de dominio, o sea a la Corporación de Asignación de Nombres y Números de Internet, más conocida por ICANN, en relación a cuestiones derivadas de la colisión entre los nombres de dominio y los derechos de propiedad intelectual.

En diciembre de 1998 se publicó un Informe provisional en el que figura el proyecto de recomendaciones, estando actualmente el Informe Final que se presentó a la ICANN, del cual vamos a ver los puntos más importantes.

A) Se comenzó adoptando prácticas normativas para el registro de los nombres de dominio de nivel superior genéricos que reducirán la tensión que existe entre los nombres de dominio y los derechos de propiedad intelectual. Asimismo se tratará que los datos de los titulares de los nombres de dominio sean los mismos de los derechos de propiedad intelectual.

   Cuando se constate que son inexactos o poco fiables los datos, y que no se puede establecer por su conducto contacto con el titular de un nombre de dominio, un tercero podrá presentar una notificación a este respecto al responsable. Si se verifica independientemente la posibilidad de establecer contacto, se podrá solicitar al registrador que cancele el registro del nombre de dominio.

B) Se recomienda que se limite el alcance del procedimiento administrativo a los casos en los que se dé la mala fe, en los que se dé el registro abusivo de nombres de dominio que infrinjan derechos de marcas.
   El procedimiento administrativo será rápido, y se realizará en línea en la mayor parte. Se limitará a la anulación o la transferencia de registros de nombres de dominio y la atribución de los costos del procedimiento a la parte perdedora, en estos costos no incluyen los honorarios de los abogados. Los órganos de registro harán respetar las decisiones en virtud de la política de solución de controversias.

C) Cuando sean marcas famosas o notoriamente conocidas se tratará de introducir un mecanismo por el cual el titular de ésta pueda obtener la exclusión de todos o algunos de los dominios de nivel superior genéricos del nombre de la marca, allí donde la marca sea famosa o notoriamente conocida con amplia base geográfica y en relación con distintas clases de bienes y servicios. Así toda persona distinta del titular no podrá registrar esa marca como nombre de dominio.
   Esta protección toma como base el Convenio de París para la Propiedad Industrial y los Acuerdos sobre Derechos de Propiedad Intelectual para el Comercio.
   Debemos tener en cuenta que no solo es para el nombre exacto de la marca famosa o notoriamente conocida, sino que debería constituir una presunción probatoria en el procedimiento administrativo, una vez fuera concedida la exclusión.

D) En los últimos años se han dado numerosos casos de registro abusivos de nombres de dominio y ha provocado la confusión del consumidor y ha mermado la confianza que merece Internet al público. Esto puede evitarse mediante la adopción de las prácticas de registro mejoradas, el procedi-

*miento administrativo de solución de controversias y el mecanismo de exclusión que se recomien*dan en el Informe final del Proceso de la OMPI.

IV. TRATAMIENTO DE LOS NOMBRES DE DOMINIO EN LOS PAISES DEL MERCOSUR

IV. 1. Argentina

Como en todos los países del planeta, Argentina no queda fuera de esta controversia y resuelve los problemas existentes entre la colisión de las marcas con los nombres de dominio que se registran de la siguiente forma:

- Establece dentro de su política que el Administrador del dominio no se hace responsable de conflictos que pudieran surgir entre los nombres de dominio y las marcas originados a partir de reservas de nombres de dominio. La responsabilidad corresponde íntegramente a la entidad solicitante.

- La entidad solicitante se hace responsable al solicitar un nombre de dominio, de cualquier conflic*to u ofensa que pueda surgir con alguna otra entidad, en cuanto al uso de nombres que represente*n marcas o identifiquen a otra entidad o a productos y/o servicios ofrecidos por otros.

IV. 2. Brasil

En el Brasil el Comité Gestor Internet do Brasil (fue creado por la Resolución Interministerial MC/MCT 147/95, publicada en el Diario Oficial del 31.5.95), delegó la administración del dominio .BR, por Resolución 001 del 15.4.98, a la Fundacao de Amparo a Pesquisa do Estado de Sao Paulo.

Esta Fundación establece que para el registro de un nombre de dominio se debe como primer paso firmar un acuerdo entre las partes, o sea entre el solicitante de la registración y el administrador del dominio (Fundación).

En este acuerdo se estipulan los derechos y obligaciones del requirente y los derechos y obligaciones del requerido. A vía de ejemplo tenemos:

I. DEBERES DEL REQUIRENTE:

- *mantener sus datos registrales actualizados*
- enviar documentación solicitada por el administrador
- mantener los servidores DNS delegados de dominio funcionando correctamente conforme a la política de la organización administradora del dominio

II. DERECHOS DEL REQUIRENTE:

- *Tramitar el registro del dominio, utilizando el sistema dado por la entidad administradora*
- Cancelar el registro, transferir su titularidad de acuerdo con los procedimientos estipulados por el administrador

III. DEBERES DEL ADMINISTRADOR:

- Mantener la base de datos, conteniendo los datos del registro

- Cancelar el registro y todos los actos del registrado desde el momento en que se constate la irregularidad en relación a las estipulaciones del administrador.

IV. DERECHOS DEL ADMINISTRADOR:

- Cancelar o no aceptar el pedido de registro, cuando sea contrario a las normas estipuladas por la organización administradora.
- Cancelar el pedido de registro cuando no se acompañe la documentación requerida

- No aceptar el pedido de registro o cancelarlo posteriormente cuando se trate de nombre no registrable, o sea aquel que sea reservado o atente contra las buenas costumbres y la moral.

Se manifiesta que la responsabilidad del nombre de dominio es entera del requirente y que al aceptar el acuerdo electrónicamente, exime al administrador de toda o cualquier responsabilidad por daños y perjuicio, respondiendo por cualquier acción judicial o extrajudicial que derive de la violación de derechos o de perjuicios causados a otros y asumiendo las penas que se originen de estas acciones.

Se cancela el registro por las siguientes causales:

- Renuncia expresa del requirente

- Por no cumplir el registrado con su deberes

- Por orden judicial.

Se fija como jurisdicción el Foro da Fazenda Publica de Sao Paulo para la solución de las controversias o dudas que se puedan dar en cuanto a este acuerdo.

Luego que la persona que quiere registrar el nombre de dominio ha leído el acuerdo antes detallado, debe tener la certeza que ese nombre que ha elegido ya no está registrado, reservado por el Comité Gestor o es una marca notoria estipulada por la OMPI, si de la búsqueda que realiza en el sistema resulta que ese Dominio es Inexistente podrá ser registrado, en caso contrario no se registrará.

Para registrar un dominio es necesario ser una entidad legalmente establecida en Brasil como persona jurídica o física que tenga un contacto en territorio nacional.

Asimismo se especifican cuales son las reglas sintácticas que debe seguir el dominio.

IV. 3 Uruguay

En nuestro país desde 1990 se realiza la administración del dominio UY así como los subdominios, por el Servicio Central de Informática Universitario (más conocido por Se.C.I.U.) de la Universidad de la República Oriental del Uruguay.

Desde el comienzo esta administración ha sido realizada sin mayores problemas, ya que no han surgido controversias entre los nombres de dominio registrados y las marcas existentes en el país.

Actualmente se está procediendo a una nueva puesta a punto de las directivas para el registro en Internet.

Cómo establecemos cuáles son los nombres de dominio que se pueden aceptar?, Cuáles los que no van contra el orden público, las buenas costumbres?, Cuáles los que no son marcas conocidas ni notorias, eso si resultaría obvio, pero es tan así?.

Todavía no ha surgido ninguna controversia, pero debemos dejarnos estar y esperar que pase?, Quién es el responsable, el que solicita, el que lo registra, la entidad encargada de esa administración?.

Como vemos mientras se llega al fin de este proceso, lo más que tenemos son interrogantes, las cuales no tienen una sola respuesta, sino que varias y todas con certeza, por lo que la entidad encargada en nuestro país de la administración de los dominios ha tomado como políticas generales de administración las siguientes:

- Como primer punto el Servicio Central de Informática Universitario se adjudica el derecho a dejar *en suspenso la delegación de la administración* de nombres de dominios, si considera que él puede entrar en colisión con las normativa en estudio.

- Una vez puesta la normativa en vigencia se evaluarán las solicitudes que hubieran quedado en suspenso.

- Se establece que la longitud total del dominio no deberá exceder los 26 caracteres, siendo caracteres válidos los números, letras y guión, no pudiendo comenzar o terminar el nombre de dominio por un guión (no se especifica si la cantidad de caracteres incluye también el dominio de segundo nivel o no, como lo estipula en sus reglas el administrador de Brasil)

- También se indica que no se considerarán para su registración las denominaciones contrarias a la moral y las buenas costumbres (*nada se dice del orden público)*
  Asimismo se deja claro que en caso de existir controversias entre un tercero y el titular del nombre del dominio que está registrado por su titularidad, el organismo registrador acatará sin más trámite la resolución de la autoridad legal competente, retirándolo definitivamente de su base, previa notificación con un plazo de 15 días al responsable del nombre de dominio.
  Se estipula como otras causales de eliminación del nombre de dominio del registro:

- La voluntad expresa de la persona responsable del dominio (solicitante, técnico, registrado).

- Por la utilización inapropiada de los dominios no comerciales
  Nada se estipula sobre la responsabilidad en cuanto a daños y perjuicios a terceros, es decir si el administrador es responsable o no por haber registrado ese nombre de dominio, o se deslinda de toda responsabilidad como lo hace el administrador argentino, nada se dice que hacer si la disputa no es en sede legal sino sede administrativa, o qué sucede si la controversia se resuelve en la vía extrajudicial.

V. CONCLUSIONES

Los Informes de la OMPI, las políticas que sigan los países del mundo con respecto a la colisión que pueda existir entre las marcas y los nombres de dominio son para evitar las situaciones de confusión en el tráfico mediante la protección del consumidor.

El uso de una marca como nombre de dominio constituye una violación del derecho exclusivo a utilizar esa marca en el tráfico económico que tiene el titular de la misma y la misma puede inducir a error a los consumidores.

Tanto los derechos reconocidos por la legislación de marcas como los de competencia desleal pueden ser afectados por los nombres de dominio.

Ante quién se recurre un acto de denegación de la inscripción de un nombre de dominio, o su registro, es un acto administrativo y como tal, susceptible de todos los recursos correspondientes a esa jurisdicción?, cuál es la jurisdicción competente en el caso de que esta actividad produjera daños a los particulares?.

Como vemos quedan muchas interrogantes, tanto la OMPI como los países están tratando de llegar a un acuerdo, esperemos lograrlo antes que se susciten más controversias.

VI. BIBLIOGRAFÍA

- Informe Final de la OMPI
- Global Top-Level Domain Dispute Resolution Policies en: http://www.digidem.com
- http://registro.br/info.html
- Manual Teórico Práctico de Marcas. Juan Manuel Gutierrez Carrau.
- Ley de Marcas 17011

El contrato de publicidad en Internet

Carmen Milagros Velarde Koechlin* (Perú)

I. INTRODUCCION

INTERNET se ha convertido en una herramienta necesaria para la investigación. Inicialmente utilizada por centros de investigación y universidades, posteriormente fue aprovechada por las empresas para desarrollar el comercio electrónico *business to business*. Desde aquellas épocas, son muchas las personas naturales y jurídicas que han resuelto tener presencia en INTERNET. Tal novedad se advierte cuando nos suscribimos a un proveedor de cuenta de correo electrónico, quien gratuitamente nos ofrece colocar nuestra página web. Incluso, son varios los sitios web que ofrecen al usuario alojar gratuitamente su página web. Ciertamente, los programas de creación de páginas web han sido altamente divulgados.

Sin embargo, estar en INTERNET no necesariamente nos asegura ser conocidos por los usuarios y menos aún, alcanzar un nivel de visitas aceptable. En un período como el actual, en donde el comercio electrónico busca fomentar el negocio entre empresas y consumidores finales (usuarios individuales), el colocar una página requiere de un estudio de mercado, así como de un diseño especial que permita la atracción de visitantes constantes.

Así, han aparecido diversas agencias dedicadas al desarrollo de publicidad en INTERNET, tales como AltaVoz, empresa chilena especializada en publicidad en Internet. ArteWeb, empresa mexicana o Colomweb, empresa de publicidad colombiana, por mencionar algunas. Todas ellas, anunciándose en la propia Red.

Estas empresas, que inicialmente resaltan la importancia de tener presencia en la Red -ya que ello significa contar con adelantos tecnológicos y por tanto, estar un paso adelante de nuestro competidores-, nos ofrecen un servicio de publicidad que involucra el diseño y colocación de una página web para nuestra empresa o institución. Efectivamente, la página web sirve para dar a conocer a una persona, empresa, asociación, etc., otorgando información necesaria sobre nuestras actividades. Estas páginas nos permiten también promover productos o servicios y desarrollar negocios virtuales. Claro está, el éxito depende no sólo de colores vistosos

La publicidad en INTERNET, evidentemente es distinta a la publicidad tradicional presentada en radio, periódicos o televisión. Más que contar con mensajes subjetivos o mensajes que transmitan emociones, se ofrece como un medio de transmisión de información la que muchas veces proporciona al público usuario datos sobre las actividades, productos y servicios de una empresa, invitando al público a visitar el local físico. Entonces, siendo una página web la "carta de presentación" de negocios virtuales o ya existentes, el servicio ofrecido por las agencias publicitarias debe ser exquisito, pero por sobre todo, completo, aplicando todas las etapas de la publicidad.

Por ello, consideramos que el rol de las agencias publicitarias es de suma importancia, por lo que sus obligaciones para con sus clientes deben ser estipuladas en un contrato que prevea todos los pormenores.

Debemos tener en cuenta que contar con publicidad en INTERNET significa tener un aviso exhibiéndose las 24 horas del día y hacerlo llegar a todo el mundo. Otro de los beneficios de la publicidad en INTERNET es la reducción de costos ya que se elimina el costo del papel, la impresión de trípticos o volantes, su distribución, etc. de igual modo, este tipo de publicidad permite interactuar con el usuario ya que éste puede enviar mensaje en busca de mayor información y hacernos conocer sus necesidades.

* Abogada de la Defensoría del Pueblo del Perú. Miembro del Estudio "Velarde & Velarde Abogados". Fedataria Particular Juramentada con Especialización en Informática por el Colegio de Abogados de Lima. Secretaria General del Cibertribunal Peruano. Egresada de la Maestría de Derecho Empresarial de la Universidad de Lima.

II. LOS CONTRATOS DE DESARROLLO DE PUBLIICDAD EN INTERNET

Actualmente encontramos dos formas importantes de desarrollar la publicidad en INTERNET. La primera se presenta como "renta de espacios", es decir, alguna páginas populares alquilan un espacio de su página para que un determinado usuario ofrezca su producto o servicio. El segundo medio, está referido a la "publicidad on line", es decir, al desarrollo de páginas web para empresas u otras instituciones.

Otras agencias desarrollan contratos de mercadeo en Internet, aplicación de encuestas, etc., todos ellos relacionados a la publicidad pero que a nuestro parecer, deben integrarse en un sólo servicio ya que para el éxito de una publicidad en INTERNET, no basta aplicar sólo una fase de la publicidad.

Sin embargo, cabe mencionar que el contrato plasma la voluntad de las partes, por lo que ellos libremente pueden establecer sus cláusulas, no obstante, quisiéramos mencionar algunos temas que estimamos importante colocar en todo contrato de publicidad por INTERNET.

III. PRINCIPALES MATERIAS A INCLUIR EN UN CONTRATO DE PUBLICIDAD

Todo contrato debe considerar la legislación sobre publicidad del país de la empresa. En materia de publicidad, las legislaciones coinciden en no aceptar publicidad falsa o engañosa, ni publicidad comparativa.

A) Garantizar un nivel de aceptación de la página web

La agencia de publicidad no puede simplemente ofrecer el diseño y colocación de la página web. Dado que el objetivo de la publicidad es atraer a los usuarios, la agencia está obligada a realizar las acciones necesarias para que el sitio web sí sea visitado, así como para que los visitantes continúen en dicho sitio, navegando por los otros enlaces. Por tanto, a nuestro parecer, la obligación de la empresa publicitaria es una obligación de "resultado".

B) Ofrecimiento de los principales servicios

El contrato de publicidad debe detallar los servicios completos y no dividirlos a fin de exigir a la empresa la suscripción de posteriores contratos. Salvo que las partes pacten lo contrario, las agencias publicitarias deben ocuparse de todos los aspectos del desarrollo de un sitio web. Esta prestación entonces, debiera abarcar los siguientes servicios:

- Estudio de viabilidad del proyecto: Importante es conocer el nivel de usuarios en la red y saber si la colocación de una determinada publicidad tendrá éxito o no.

- Diseño y publicación de la página web.

- Actualización constante de la página web: lo que incluye la modificación de las páginas existente, agregado de nuevas secciones, enlaces nuevos, etc. La actualización implica también un estudio del sitio web para saber si éste es visitado o no. De no serlo, establecer cuáles son las causales y realizar los agregados indispensables para hacer del sitio web un lugar más popular. Implica también mantenerlo vigente para que capture siempre el interés de los visitantes.

- Uso de una adecuada tecnología para la mejor transmisión del mensaje: se deben detallar los programas a utilizar o el tipo de servidor en donde se alojará la publicidad. Mencionar los detalles técnicos es importante ya que a veces se pierde cantidad de visitantes porque el servidor no soportó una alta carga de visitas o la página cargaba con lentitud, aburriendo al usuario.

- Verificación de los detalles técnicos: Puesta en marcha la página, es necesario evaluar el buen funcionamiento de los sistemas. para ello la empresa está obligada a contar con personal calificado.

- Creación de formularios: Con ellos se podrán realizar encuestas, recoger información o dudas de los visitantes y ofrecerles nuevos servicios según sus requerimientos.

- Instalación de autorrespondedores: este método ayuda a que, luego de recibido el correo de un visitante, se le pueda enviar inmediatamente un mensaje preestablecido para confirmar la recepción del email. Esta técnica apoya la publicidad y marketing personalizado pues el usuario se siente escuchado por la parte.

- En algunos casos, administración del sitio web.

- Colocación de servidores Web en la empresa, de ser el caso: Es muy importante el servidor donde se coloque la página web ya que no basta el simple diseño. Si el servidor no soporta mucha congestión o tráfico, entonces el sitio web a publicitar quedará sin acceso.

- Instalación y registro del dominio, de así solicitarlo el cliente.

- Dar asesoría técnica y de mercadeo.

- Promoción del sitio web para que sea fácilmente encontrado por los usuarios: Ello implica colocar el sitio en los principales buscadores y desarrollar campañas de mercadotecnia especializadas o actividades promocionales para hacer del sitio web uno de los más visitados.

C) Obligaciones de la agencia publicitaria

Deber de confidencialidad: La agencia guardará toda información entregada por el cliente y que no sea utilizada en la publicidad. La agencia debe comprometerse al uso de sistemas de seguridad para la protección de la información del sistema, es decir, protección de los datos sobre visitantes, correos y mensajes de los usuarios, información colocada en los formularios, etc.

La agencia cederá los derechos de propiedad intelectual de los documentos hechos en Internet, etc. Asimismo, tiene la obligación de enviar al cliente los formularios en el período pactado y conservar los datos en un medio permanente e inalterable.

D) Obligaciones del cliente

Por su parte, el contratante tiene la obligación de proporcionar los datos relevante de su empresa, así como la información que le interese sea colocada en el sitio web. De igual modo, debe proporcionar la información para su actualización. dicha información contempla los nuevos productos o servicios, cifras o estadísticas, etc., que estime relevante y que desee sean colocadas en la página web. La información debe ser enviada en la fecha pactada.

El cliente debe también escoger el idioma en el que desee se publique su página web. Cabe recordar que a mayor número de idiomas, mayor será el mercado y los usuarios que accedan a visitar su sitio web.

El cliente aprobará cada una de las etapas de la campaña publicitaria, permitiendo así que se continúe con la siguiente fase.

Finalmente debe pagar la contraprestación, la que puede darse según se vayan culminando las etapas de la publicidad.

IV. INTERNET DENTRO DE LA EMPRESA

El uso de la web en la empresa es actualmente conocido como Intranet y requiere también del diseño e instalación de páginas web que permitan el envío de mensajes corporativos entre los trabajadores de una empresa. Asimismo, deben ser ideales para comunicar el resultado de las gestiones, informar los avances de los diversos departamentos o áreas, por tanto, puede llegar a coordinar el trabajo de toda la empresa. La publicidad, a nuestro parecer, es también aquí muy importante, pues un diseño llamativo y de fácil uso, permitirá a los empleados el constante uso de la Intranet. También los incentivará en sus labores ya que ellos se sentirán parte de una empresa moderna con metas y aspiraciones que utiliza las nuevas tecnologías.

Participación política: de la participación presencial a la virtual (la manifestación a través de Internet)

José Vicente Cebrián / José Luis González Quirós (España)
Madrid, 13 de Marzo de 2000

En una de las grandes películas de John Ford (The last Hurrah, 1958) se nos presenta lo que tal vez sea la primera incursión del cine en el debate sobre las repercusiones decisivas que la televisión estaba comenzando a tener en la política, hasta el punto de determinar los desenlaces de las convocatorias electorales y, por tanto, de condenar a muerte a toda una forma tradicional de entender las contiendas electorales y la misma democracia.

El alcalde de la ciudad y gobernador del estado, magistralmente interpretado por Spencer Tracy, es un viejo zorro de la política, amigo de todo el mundo, populista sin exceso, trabajador infatigable y honrado. Nuestro hombre se conmueve con los problemas de la gente y lucha astuta y decididamente contra la injusticia y los abusos: en fin, un paradigma, según lo que con toda probabilidad pensaba Ford, de cómo debiera ser un político decente; alguien que ni siquiera había podido dedicar parte de su tiempo a ocuparse de su único hijo que es, a todas luces, su contrafigura, un verdadero idiota.

Pues bien, del mismo modo que el hijo desconoce los valores del padre para vivir en un mundo frívolo y absurdo, el poder político basado en la autoridad y el prestigio, en la calidad humana de alguien que es escogido por sus semejantes cercanos, va a ceder el paso a un poder que se "fabrica" contando esencialmente con las ventajas que proporciona la posibilidad de emplear la TV para crear un nuevo personaje público.

A lo largo de la película asistimos escena tras escena al buen hacer del viejo alcalde y gobernador: nada se le escapa, manda de verdad, sabe lo que hace y lo que tiene que hacer cuando algo amenaza con salirse de su sitio. Pero no puede prever algo que a la postre le retira de su magistratura y que acaba, incluso, con su vida en una metáfora muy plástica del surgimiento de nuevas formas de gobernar y de relacionarse con los electores.

Vemos como su última batalla la pierde contra un adversario insignificante y absurdo (tan memo como su único hijo), manejado por cuatro magnates bastante mangantes a los que el protagonista había podido sujetar hasta ese momento. Pero el idiota elegido penetra en las casas de todos por la ventana electrónica y consigue ser aceptado como una novedad interesante por la mayoría del electorado aunque, como es obvio, nada tiene que decir ni vale para nada. La televisión es aquí para Ford un medio que emplea la oligarquía local para sacudirse el yugo de la democracia en manos de un demócrata que lucha por una igualdad real, que, a lo que parece, no es muy del agrado de ciertos happy few.

Ford, que ha dramatizado con prontitud una novedad trascendente, ha dado una interpretación de la relevancia de la TV que ahora se nos antoja elemental. De apenas diez años antes es un testimonio ideológicamente mucho más sofisticado y de mayor alcance como metáfora antitotalitaria: 1984 de Orwell (1949).

Lo que fue visto inicialmente como un alegato antiestalinista sirvió también a Marcuse para caracterizar ciertos aspectos de las sociedades capitalistas en las que la ausencia de libertad se soporta de un modo "suave, razonable y democrático". Más allá de estas lecturas un tanto sesgadas, la metáfora del "Gran Hermano" se ha convertido en el factor común de cualquier pesadilla tecnológica, pero es también, cincuenta años más tarde, un motivo de reflexión de significación muy amplia a la luz de los increíbles desarrollos de la tecnología digital en el campo de las comunicaciones y del nacimiento de la cultura de masas que tiene en la televisión su instrumento más poderoso y su totem.

Orwell no sólo tenía a la vista las prácticas stalinistas, las técnicas de reescritura de la historia en la que los soviéticos han sido ciertamente expertos, sino que necesariamente recordaba el poder de la radio como medio de manipulación de masas que el nazismo supo emplear con maestría. Refiriéndose a ello escribió Max Horkheimer que si el nazismo hubiera dispuesto de tecnologías más poderosas tal vez su triunfo hubiera sido absolutamente inevitable.

Hay pues una tradición intelectual y crítica que ha puesto de manifiesto los riesgos de manipulación y las amenazas para la libertad que pueden significar los grandes instrumentos de comunicación, subrayando, en todo caso, el poder enorme que confieren a quienes los saben y pueden manejar. Pero, por fortuna, vivimos en un momento en el que el triunfo de la democracia política no está en entredicho. Son muchas las voces (por ejemplo: Sartori) que, sin embargo, ponen el acento en la desvirtuación que significan estos fenómenos de cultura de masas (tan radicalmente inseparables de las tecnologías que los hacen posibles) para el logro efectivo de una democracia madura.

Estas consideraciones han de ser recordadas como telón de fondo de nuestro tema toda vez que lo que ahora se trata de discutir es en qué modos (si es que es posible en absoluto) pueden darse nuevas formas de participación política y de ejercicio de los derechos democráticos que estén basadas en las nuevas posibilidades de la tecnología.

Existe ya una literatura muy amplia y no siempre homogénea sobre las consecuencias sociales, culturales y políticas que se experimentará en nuestras sociedades como consecuencia de la universalización de las comunicaciones a través de la WWW y, en general, de las novedades que van a ser posibles gracias a la tecnología digital. En lo que aquí nos importa ahora lo que parece claro es que al alterarse el marco de las posibilidades de comunicación y diálogo de las personas entre sí y entre las personas y las instituciones, existe, al menos como posibilidad más o menos utópica, la capacidad de conocer al momento la voluntad popular sobre distintas cuestiones y, en todo caso, se abren nuevos caminos de diagnóstico y consulta de las opiniones públicas y de contacto entre los electores y sus representantes, los órganos de la administración y los responsables del gobierno.

Es característico de nuestras sociedades el que la existencia de una mera posibilidad sea convertida en un deseo y, tarde o temprano, en un acto efectivo. De manera que no cabe dudar de que ya que es posible que cambien las formas tradicionales de articular la representación y la consulta popular no es muy arriesgado pronosticar que tarde o temprano lo acabarán haciendo.

Hay que preguntarse, por tanto, cuáles serán los desarrollos previsibles de estas novedades y cuáles han de ser las cautelas y normas que han de condicionar estas nuevas formas de hacer política para evitar que conduzcan por derroteros indeseables.

Las formas de comunicación (y consecuentemente, las formas políticas) han dependido siempre de las tecnologías disponibles: desde el desarrollo del habla humana (tan variada como siempre comprobamos los que carecemos del don de lenguas), hasta Internet, pasando, desde luego, por la imprenta, las formas en que las personas nos entendemos han estado condicionadas por las tecnologías disponibles.

La democracia, por ejemplo, que era posible en las ciudades griegas de pocos habitantes (Platón consideró que más de muy pocos millares de personas era número indeseable) era inconcebible en el Imperio de Alejandro. Tecnologías y políticas no han cambiado, sin embargo, al mismo ritmo. Ahora la tecnología va por delante, sobre todo en la medida en que la forma política de las democracias parlamentarias estaba ya consolidada (en cuanto a modelo) incluso antes de la existencia del teléfono. Hoy sería concebible, desde un punto de vista tecnológico, que todos eligiésemos al Presidente de los Estados Unidos, lo que seguramente es algo prematuro, políticamente hablando.

Lo que ahora tenemos es un sistema infinitamente más poderoso de comunicaciones, pero, precisamente por ello, hemos de orientarnos en medio de un sistema infinitamente más complejo de signos. Las preguntas que deberíamos hacernos suenan un poco raras, porque hace tiempo que creemos haber llegado a la perfección política (esa es la idea del fin de la historia) y, por el contrario, somos conscientes de estar entrando en una aceleración tecnológica bastante impredecible.

Pues bien: ¿Podremos seguir haciendo políticas del siglo XIX con tecnologías del siglo XXI? ¿Hemos de hacer políticas distintas sólo porque podamos gozar de tecnologías más poderosas? ¿Puede adaptarse la forma democrática imperante en las últimas décadas del soporte de papel a sociedades en que se habrán impuesto

otros soportes (no preocuparse -salvo los ecologistas- el consumo de papel seguirá creciendo como lo ha hecho desde los comienzos de la informática) más inmateriales?

Para ver que podemos ir diciendo sobre estas cuestiones habrá que partir de dos puntos en cierto modo opuestos: en primer lugar de las restricciones que la idea misma de democracia pueda imponer a los nuevos desarrollos y, en segundo lugar, de las experiencias, aún inciertas y tentativas pero ya abundantes, de lo que podríamos llamar democracia electrónica (es evidente que democracia digital tendría resonancias indebidas, al menos para los españoles de cierta edad).

1. Restricciones políticas a las nuevas posibilidades tecnológicas en el campo de la participación y de la expresión de la voluntad popular.

La ventaja esencial que sería oportuno poder aprovechar de las nuevas tecnologías de comunicación consiste en que, por lo pronto, ahora podemos ser no sólo protagonistas pasivos de un proceso público de comunicación, sino elementos activos de un intercambio mucho más complejo y difícil de analizar, llegar al emisor de los mensajes de un modo que ahora llamamos interactivo y sin que apenas sea necesario un determinado lapso de tiempo entre la recepción y la respuesta: ¿para qué puede servir esto?

En primer lugar, se hace necesario recordar las limitaciones que la democracia impone en cuanto al lugar y en cuanto al tiempo como requisitos previos de la posibilidad de la democracia misma. No hay democracia sin censo y no hay democracia sin fechas de consulta, períodos de campaña etc.

Ahora bien, la primera de las limitaciones de las que podemos prescindir con la nueva tecnología es, precisamente, las del espacio y el tiempo. El internauta es un ser esencialmente deslocalizado, un habitante de "nowhere" y que también juega, por ello mismo y a su modo, con el tiempo. Esta condición tiene realmente poco que ver con la del habitante censado, a no ser que prosperen los intentos de ciertas multinacionales de tenernos a todos en lista, pero esta es otra cuestión.

Una dificultad que derivaría, seguramente, de este primer tipo de cuestiones es la que tiene que ver con la ya existente inadecuación entre los períodos necesarios para una reforma política importante (por ejemplo: la del sistema educativo o la de las aguas, etc.) y los ritmos cada vez más cortos de convocatorias electorales. La precaución de los políticos frente a las campañas a la hora de tomar medidas impopulares se elevaría al paroxismo con algo que se pareciese a un refrendo cotidiano.

Por cierto que nada sería más fácil que la desaparición de la idea de la responsabilidad del político que se convertiría en un mero ejecutor de voluntades expresas, volubles y terminantes. Nada que ver, por tanto, con la idea de representación. Podríamos llegar al mapa de Borges, al mapa que coincide con lo representa y que, por ello mismo, ya no es un mapa de nada.

En segundo lugar, habría que considerar que, aun superando los obstáculos del tipo anterior, habríamos de bregar con el hecho de que, en general, la generalización de derechos ha sólido traer consigo un cierto retraimiento práctico.

Para ciertos observadores, el marco de la democracia se ha convertido en su único contenido efectivo, de manera que se podría llegar a decir que la democracia ha pasado de ser un ideal más o menos emancipador a ser una instancia de legitimación de un cierto estado de cosas, un medio de cercenar la novedad, el cambio y, por supuesto, todo lo que pueda asimilarse, más o menos, a lo que antes se llamaba la revolución.

Esta clase de diagnósticos se complicaría con la aceptación de nuevas formas de recuento y control dado el hecho, bastante poco discutible, de que el conjunto de caracteres que describimos como pluralismo-anomia-relativismo son universales y no facilitan precisamente la existencia de ciertos consenso básicos que han de ser sostenidos, más bien que por su aceptación popular, por pactos de políticos.

La idea del estado-nación (y sus similares) sufriría fuertes embates en todo caso, lo cual acaso sea bueno, acaso no.

El voto expresa participación y, también y tal vez sobre todo, legitimación, control y cambio. Popper, consecuentemente con su idea de lo que es el conocimiento y lo que es la discusión racional, caracterizó muy razonablemente a la democracia como la posibilidad de derribar gobiernos sin derramar sangre. Todas estas funciones se alterarían, seguramente de modo distinto, pero variando en todo caso como tal vez tengamos ocasión de ir viendo en las próximas décadas.

Bell subrayó hace tiempo como rasgo dominante de las sociedades democráticas la ausencia de una adhesión normativa a un hogar público, es decir de una filosofía política que medie entre los conflictos privados cada vez más complejos e irreducibles a una única dimensión. Esa ausencia es especialmente grave a la hora de poner en pie nuevas formas de vida política sin que quede claro que baste la mera posibilidad para considerarlas en serio.

No es fácil saber qué pasaría si, en nombre de una voluntad popular perfectamente definida, comenzamos a cambiar a ritmo no de responsabilidad sino de impulso por el deseo y la novedad. Para Tocqueville, el aspecto característico de la modernidad era el hecho de que "la trama del tiempo se rompe a cada instante, y se borra la huella de las generaciones" y, en ese sentido, nada más moderno que el tipo de galaxia comunicativa en el que ahora estamos entrando en el que la información (que en dosis masivas es muy difícilmente discernible de la desinformación) bien puede ahogar al buen sentido.

¿Acertaremos a librarnos de todo ello, a evitar las amenazas y a encontrar nuevas utilidades positivamente valiosas a las posibilidades abiertas y que se abrirán por tecnologías que ahora ni siquiera podemos imaginar apenas? No es poco plantearse la cuestión y parece imprescindible hacerlo antes de dar el más mínimo paso.

Veamos, en segundo lugar, lo que nos dice la experiencia, aunque teniendo en cuenta que nos hallamos, tan sólo, en el umbral de lo que podrá ser una verdadera invasión de innovaciones cada vez más sofisticadas y cada vez más desafiantes, si es que estamos decididos a aprovecharlas para mejorar la calidad de nuestras instituciones aprovechando todo lo que se nos ofrece.

Se trata, por tanto, de experiencias muy preliminares que se centran, sobre todo, en el diálogo entre administradores y ciudadanos, en la disponibilidad de las fuentes de información y en la apertura de nuevos canales de participación. No cabe duda, sin embargo, de que estas innovaciones retratan a las sociedades que las implantan, y que, en la medida en que exista una voluntad política decidida de avanzar en la implantación de la Sociedad de la Información, el papel ejemplar y dinamizador de las administraciones y servicios públicos es esencial.

La Sociedad de la información progresa a lomos de ideas, no de simple acumulación de aparatos, líneas o sistemas. Y la mejora de las relaciones entre ciudadanos y administración puede y debe ser uno de los hilos conductores hacia esas formas nuevas de socialización.

2. Experiencias de nuevas formas políticas de la democracia electrónica

La única pretensión de este apartado es comentar algunos de los ejemplos mas conocidos, al menos hasta el momento de escribir estas lineas, de utilización de la tecnología electrónica en las formas y modos de participación democrática, citando con cierta frecuencia ejemplos españoles, por ser los que mejor conocemos.

Obviamente existen otros ejemplos, distintos a los que aquí se citan, que pueden parecer mejores, más populares o más importantes, a quienes los conozcan. No hemos tratado de ser exhaustivos, sino de aportar realizaciones practicas, que puedan servir para aumentar el conocimiento en la materia, que muevan a la reflexión política y eventualmente animen a llevar a cabo experiencias similares.

Aún a riesgo de simplificar el fenómeno, podríamos indicar tres grandes bloques de realizaciones que responden a finalidades distintas pero que perfilan unas tendencias en la búsqueda de nuevas formas de participación.

Esos tres bloques se refieren a las nuevas formas de informar, de administrar y, finalmente, de procurar una mayor participación en la vida política y democrática de una comunidad. Se establecen así tres grandes clases en este campo, en el que la información aparece como un requisito consustancial a la libertad, y por lo tanto al ejercicio de la democracia.

El análisis de estas formas nuevas de participación nos hace ver experiencias bienintencionadas, pero aisladas de un marco más general, no llegan a fructificar, al faltarles un apoyo firme cuando está ausente la decisión política de ampliar los procesos de participación, de control y de toma de decisiones.

Con todo, ello no quiere decir que experiencias de este tipo no deban de continuarse, pero debe de prestarse un interés especial al mantenimiento del proceso en su globalidad, como línea de avance con mejor probabilidad de éxito.

Si comenzamos por el campo de la información, las tecnologías que conforman las nuevas formas de comunicación suponen un avance espectacular en las posibilidades de información al alcance del ciudadano. Nos estamos refiriendo claro está al fenómeno Internet, que si no es el único dentro de estas tecnologías, si constituye el mejor paradigma existente.

En primer lugar por que permite que los ciudadanos tengan un acceso eficaz y a un coste asequible a una enorme cantidad de fuentes a lo largo y ancho de todo el mundo, y prácticamente sin limitación de ideologías, culturas o formas políticas diferentes. Podríamos decir que únicamente no está en Internet quien no quiere estar, por las razones que sean.

Por primera vez en la Historia, la globalidad, por utilizar una expresión al uso, es una posibilidad real de la que pueden beneficiarse los ciudadanos de forma individual, sin exceso de intermediarios y a su voluntad. Con ella, aparece la posibilidad de incrementar la memoria disponible de modo inmediato. La información no sólo está disponible, sino que puede acudirse a ella sin las restricciones que el coste en tiempo supone para otras formas de acceso menos tecnológicas.

Finalmente, hay que referirse a la posibilidad de participar, de no ser exclusivamente sujeto pasivo de la información. Entendiendo esto en el doble sentido de poder fácilmente responder a una determinada información y de poder, de manera real y no teórica, informar de las propias ideas.

Lo primero supone un cambio substancial ante las formas tradicionales de los medios de comunicación, concebidos prácticamente como focos emisores de información ante colectivos que actuaban como receptores pasivos. Lo segundo rompe las barreras de hecho tanto económicas como técnicas que existían para poder comunicar las propias ideas.

Aparece así la demanda de una nueva fuente de información, tradicionalmente opaca para el ciudadano, pero básica para una participación efectiva del mismo en la gestión de su comunidad política. Nos referimos a la información administrativa, al inmenso conjunto de datos, estudios, informes, propuestas y actuaciones de todo tipo que constituye la vida diaria de cualquier administración.

Y es aquí, una vez más, donde aparecen las primeras diferencias entre los países, diferencias clamorosas, diferencias de actitud, diferencias por lo tanto políticas, y fruto sin duda de diferentes culturas políticas y de diferentes apreciaciones de los valores democráticos.

Diferencias entre aquellos países, la mayoría de corte anglosajón que creen en el derecho a la información como una necesidad para el conocimiento y la posterior participación, y los que viven anclados en formas tradicionales pero poco democráticas.

Si en los primeros esta convicción se plasma inicialmente en las Leyes de Derecho a la Información, cualesquiera que sea su nombre, las nuevas tecnologías han supuesto la posibilidad de impulsar de forma espectacular por las propias administraciones el ejercicio de este derecho.

Las administraciones de corte anglosajón, la norteamericana, la canadiense, la inglesa, e incluso aquellas que nos suenan desde Europa algo exóticas, como la australiana o la neozelandesa, son ejemplos a seguir, por gran número de países europeos y sin duda por España.

Los ejemplos de los Estados Unidos son casi inabarcables. Desde la Casa Blanca o los distintos departamentos ministeriales, los Gobiernos estatales o locales, las organizaciones de todo tipo, las empresas, las universidades, los medios de comunicación tradicionales e incluso las numerosas religiones y sectas, toda la sociedad norteamericana, realiza esfuerzos notables para proporcionar información a través de Internet.

Por citar algunos casos más notables, el Departamento de Defensa, el Estado de Pennsylvania, con su dirección Internet en la matricula de los coches, la CNN, la Fundación Getty, en un notable esfuerzo de promoción cultural, y sin duda la librería "virtual" Amazon en el aspecto comercial.

Junto a ello un panorama más gris en gran parte de Europa y un panorama ligeramente desolador en el caso de nuestro país. La Unión Europea, a través del programa ISPO (Information Society Promotion Office), proporciona información sobre un gran número de proyectos.

En el caso español, la inexistencia de información es el simple reflejo de una administración posesiva, desconfiada, temerosa de un administrado informado, poco proclive al servicio público en el sentido más directo de la expresión, muy paternalista sobre lo que al ciudadano medio le puede o no interesar, y poco democrática en cuanto a la obligación de informar como elemento básico que permite la acción política.

Asistimos así al reino de lo obvio y lo superfluo. En general la información administrativa es muy pobre, y se tiende mas a criterios de propaganda que a suministrar información real. Todo ello viene a reflejar la falta de una acción política real sobre el tema, a diferencia del trabajo que se viene realizando por otros gobiernos europeos, incluida la propia Comisión.

En este contexto hay que mencionar positivamente la Jornada sobre la Sociedad de la Información, impulsada por el Ministerio de la Presidencia y en la que estuvieron presentes Fomento e Industria y otros miembros de la Administración. Consecuencia directa de la misma, ha sido la aparición a finales del pasado mes de Diciembre del proyecto conocido como INFO XXI que de momento se encuentra en estado de buena esperanza. El impacto que las pasadas elecciones ha tenido sobre su fulgurante aparición y escaso contenido es bastante evidente.

Como elemento positivo hay que destacar la adecuada información sobre el Consejo de Ministros, aunque de localización casi imposible, y que contrasta con la información tardía y no muy buena sobre las ruedas de prensa posteriores. Contraste aún mayor al estar situada dicha información dentro de las páginas de La-Moncloa, construidas siguiendo el éxito de las de la Casa Blanca, sobradas de propaganda burocrática, y que, en muchos casos, ni siquiera enlazan con las de los respectivos departamentos, en una muestra de desidia, que se repite incluso entre organismos de un mismo Ministerio.

Dentro de este casi desierto, aparecen algunos elementos destacados como las páginas del Senado y del Congreso, donde podemos encontrar los resúmenes de los distintos trabajos en Comisiones, Plenos, etc. Esta información, aunque de aparición tardía, al ser gratuita, rompió un abusivo sistema de venta de los respectivos Boletines en su formato tradicional.

Hay que citar necesariamente la demanda insatisfecha de obtener de forma también gratuita el BOE, que por razones desconocidas, y seguramente nada edificantes, se sigue negando. La suposición de que, al no ser una demanda numéricamente importante, no debe de ser satisfecha de forma gratuita, añade tontería a la falta de sensibilidad.

Se podrían citar otras páginas, como las del Ministerio de Administraciones Públicas que junto a la Secretaria General de Comunicaciones, intentan liderar la llamada Sociedad de la Información, frente a los intereses del Ministerio de Industria, o las de la Guardia Civil, con un diseño enormemente cuidado, una actualización muy frecuente y un elevado nivel de audiencia.

Para terminar este apartado hay que citar aquellos casos en los que las nuevas tecnologías permiten conseguir unos ciudadanos mas informados a pesar de los esfuerzos para evitarlo de sus propias administraciones. Tiannamen, Chiapas, Sarajevo, Kosovo son ejemplos bien conocidos. La mayoría se refieren a la denuncia de situaciones no democráticas e incluso trágicas, y otros muchos son reflejo de organizaciones activistas de todo tipo.

Otras veces simplemente permiten romper un silencio informativo fruto exclusivamente de elevar el autismo a la categoría de paradigma del comportamiento político. En España, ante la ausencia total de información oficial en la Red sobre el conflicto de Kosovo, las estadísticas denuncian un aumento espectacular de accesos a informaciones provenientes de otros países.

Veamos rápidamente el panorama de la segunda de las actuaciones, las nuevas formas de realizar las tareas administrativas. El intento de construir una administración más eficaz y más cercana al ciudadano, como elemento previo de una mayor participación en la vida de la comunidad.

Hay que destacar como notable el ejemplo del gobierno inglés, fuertemente empeñado en la tarea, tanto de forma directa, a través de sus ministerios como promoviendo actuaciones en gobiernos regionales y locales. Los proyectos "Better Government" e "IT for All" son las realizaciones más destacadas.

Proyectos similares se han abordado por las administraciones de Suecia, Dinamarca y Canadá, y con mayores limitaciones en los Estados Unidos, Francia, Japón y Corea.

En el caso español hay que citar la experiencia de InfoVille en Villena, Valencia, de corte fuertemente socialdemócrata en su concepción y desarrollo, y por lo tanto de difícil extensión a otras administraciones, incluso de la misma Comunidad.

En la administración tributaria, la reciente experiencia del pago del IRPF aparece curiosamente como un posible ejemplo de la llegada de una nueva amenaza, la "cyberburocracia". En efecto, efectuar la declaración de la renta por Internet supone mas procesos administrativos y acudir a mas lugares de lo que supone el procedimiento tradicional.

Una característica que suele ser común a todos estos esfuerzos, en casi todos los países, es la falta de una información y evaluación adecuada sobre los resultados. Y cuando existe suele provenir de las propias administraciones, que tienden lógicamente a magnificar los logros. La principal excepción a esta regla se encuentra otra vez en los países anglosajones. El Reino Unido para asegurar la seriedad de su proceso, acaba de publicar un documento reconociendo las dificultades, y en consecuencia proponiendo medidas correctoras, siendo una de ellas el alargamiento del proyecto inicial, que lejos de terminarse en el año 2002, no se espera que finalice hasta el 2008.

Llegamos así al tercer elemento, el impulso directo a estas formas de participación democrática. La mayoría de los proyectos se refieren también a la participación a través de formas mas o menos cercanas al Internet, pero antes de estudiarlas vamos a comentar brevemente algunas experiencias de votación electrónica.

Un cierto atractivo tecnológico ha inducido a buscar la introducción de este tipo de elementos en el propio proceso electoral. Curiosamente, no se suele buscar una mejora del propio proceso, sino del sistema posterior de recuento y de información de los resultados. Existen algunas experiencias, tanto en el País Vasco como en algún país Iberoamericano, y muy recientemente en Estados Unidos, pero difícilmente podrán superar las lógicas suspicacias de la opinión pública.

Una variante de este método es la propuesta del colectivo "Build South Africa", un grupo independiente, radicado en Londres y que propugna que los aproximadamente 400.000 sudafricanos residentes en el Reino Unido puedan votar en las próximas elecciones a través de Internet.

La limpieza de la votación electrónica estará siempre bajo sospecha, ante la imposibilidad de su control por los ciudadanos. El manejo que de la información de los resultados suelen realizar los gobiernos, incluso en elecciones sin sombra de alteración de resultados, no contribuye, precisamente, a aumentar la confianza.

Es dificil, al menos en el actual estado de la técnica, que se pueda obtener un proceso transparente. Si ya actualmente, los procesos electorales de muchos países adolecen de poca cultura democrática, pensar que esta vaya a aumentar por usar tecnologías no tradicionales nos acerca peligrosamente a Husley y su "Mundo Feliz".

Una posible solución estaría en dirigir los esfuerzos tecnológicos no al proceso de votación propiamente dicho, sino al del recuento y publicidad de los resultados. Este último punto suele resolverse por los propios partidos políticos y por los medios privados de comunicación. Para el primero, aunque existe la tecnología adecuada, será necesario realizar algunas experiencias.

Volviendo al campo de la participación, podemos distinguir dos tipos de experiencias. Una que llamaríamos indirecta, promovida por Fundaciones y sociedades de estudio y que promueve una participación un tanto de laboratorio. La sociedad norteamericana, rica en este tipo de organizaciones es la que cuenta con mayor número de proyectos, la mayoría mas dedicados a la promoción de legislación sobre derechos y libertades que al fomento directo de la participación a través de la Red.

Entre los ejemplos más conocidos pueden citarse The Loka Institute, el Center for Democracy and Technology, y merece la pena destacar el proyecto de ámbito local Minnesota e-Democracy, por la variedad y amplitud de su contenido.

Llegamos así a los proyectos más interesantes políticamente, que son aquellos que promueven la participación directa de los ciudadanos, o al menos de un cierto colectivo social.

Volviendo a citar al Reino Unido, el UK Citizens Online Democracy (UKCOD) es quizas el primer proyecto europeo en este campo, y sin duda uno de los mejores por su concepción y desarrollo. Desde 1995 y a partir del trabajo de 12 voluntarios y unos 200 colaboradores, han venido experimentando formas de participación en diferentes proyectos propios, y colaborando en la implantación de otros proyectos.

Sus tres niveles de participación, público en general, políticos, e invitados, junto a la aportación de información que proporciona el grupo de soporte, constituyen un modelo de organización para este tipo de foros.

La Unión Europea solicitó su participación en la campaña sobre la posible integración inglesa en el euro, asi como el propio gobierno inglés para la creación del proyecto de "Better Government" antes citado. Asimismo los proyectos de Norwich y Brent han contado para su diseño con la colaboración de este grupo. Otro grupo destacado es Nexus, cercano al Partido Laborista y configurado como una estructura mas elitista de grupos de trabajo.

En el área de proyectos locales, destaca la experiencia del Norwich City Council que promueve un proyecto llamado "Norwich Connect". El programa Community Power, lo forman doce grupos con una formación previa, y que pueden participar en la toma de decisiones del Ayuntamiento. Los grupos se forman con sus propios miembros y con vecinos voluntarios. Cada grupo se organiza de modo diferente, bien en reuniones abiertas, cerradas, envío de circulares, etc.

Han obtenido progresos importantes en el campo de la información. Llevan dos años de trabajo y consideran que su impulso proviene de las necesidades, y no de las tecnologías. Entre otras cosas proponen dotar de correo electrónico e incluso videoconferencia a todos los concejales para reducir el papeleo y aumentar la co-

municación, colocar puestos públicos, etc., aunque de momento sus principales éxitos están en el campo de la información.

Otro proyecto notable es el de la ciudad de Gothenburg, que comenzó hacia 1990 el proyecto DALI (Delivery and Access to Local Information and Services). DALI proporciona información local y la opción de participar en debates sobre política local. Participan tres distritos con unos 15.000 habitantes cada uno y cuatro políticos locales por distrito. La evaluación indica un éxito moderado. Tienen unos 40 accesos por distrito y día, y han realizado una docena de debates, la mayoría entre los propios políticos.

Como ejemplo de debates se puede citar la discusión sobre si el sistema se puede utilizar para información comercial, o solo administrativa, al estar financiado en su totalidad por fondos públicos. De momento esta última es la postura que prevalece. Otro debate se refiere a la protección de la intimidad al publicarse documentos de la administración.

Un tercer ejemplo, llamado "21 Aust" está actualmente en desarrollo en Australia. Está formado por tres líneas diferentes de trabajos: una Convención Virtual que realiza debates sobre la Constitución, un foro sobre Democracia On-Line, y otro foro con temas de contenido social. Incluye además una amplia colección de direcciones y de referencias documentales, acerca del tema.

En todas las experiencias se puede observar que los debates son supervisados en su desarrollo, que no en su contenido, de modo similar a lo que ocurre en los debates de los Parlamentos. Adicionalmente se ha podido comprobar la dificultad de dirigir este tipo de debates, ante la distancia que crea el ordenador.

Un caso digno de estudio es el proyecto del Senado español que comenzó a mediados del mes de abril de 1998, en el marco de la llamada Comisión Internet. Una iniciativa notable y que desde luego merece un reconocimiento público, aunque su desarrollo no esté siendo a nuestro juicio muy afortunado.

El proyecto tiene dos apartados distintos. Uno está formado por las diferentes comparecencias de personalidades relacionadas con dicho fenómeno Internet, y cuyas intervenciones se publican en las páginas electrónicas del Senado, si bien hay que decir que con notable retraso, lo que hay que achacar a la inadecuación del soporte administrativo.

El otro, más interesante desde el punto de vista político lo constituye un foro de debate público. Por razones desconocidas, seguramente el propio desconocimiento del sistema, no se ha querido un debate organizado, lo que muy pronto ha desembocado en falta de interés por el propio foro.

Sin embargo un análisis detallado de su desarrollo permite obtener algunas conclusiones. La primera y mas singular es la nula participación de los propios senadores. Salvo algún caso aislado, los miembros de la Comisión no se dignan participar en el foro. Al parecer se ha buscado expresamente esta no participación, aunque la razónes que se dan para ello no son muy claras y se acrecienta la sospecha de falta de interés o de precaución ante una expresión libre de las opiniones.

Dos lecciones pueden sacarse de la experiencia. La necesidad, por otra parte conocida, de regular los debates, y especialmente la necesidad de que los políticos directamente interesados participen en ellos.

Cabría citar otros ejemplos pero no aportarían mucho a lo ya expuesto. Para concluir este apartado con una referencia más directa a nuestro caso habría que subrayar lo siguiente:

El conjunto de la administración española está lejos de haber asumido su obligación de informar a los ciudadanos y, menos aún, de incorporar nuevas posibilidades tecnológicas para facilitar el ejercicio de los derechos teóricamente vigentes en esta clase de cuestiones. Sería necesario, pues, promover mecanismos formales para que este derecho pueda ejercerse de manera eficaz y a la altura de las posibilidades que actualmente nos brinda la tecnología.

Debe de establecerse un plan concreto de proyectos y realizaciones específicas para ofrecer a los ciudadanos información proveniente de los diferentes departamentos de la administración, cualesquiera que sea su nivel, y promoverse proyectos pilotos en todos los departamentos de la administración central que permitan ensayar nuevas formas de relación administrativa.

Análogamente deben de estimularse proyectos de participación, no necesariamente desde el campo de las administraciones, sino acudiendo a toda clase de organizaciones políticas y sociales, favoreciéndose desde la administración la financiación de estos foros de debate. Dichos foros deben de estar planificados y dirigidos, contando a ser posible con la participación de ciudadanos y de políticos o de responsables administrativos.

Cuantos estamos convencidos de que vamos hacia algo que puede ser excelente o mediocre según el empeño y la inteligencia que pongamos en ello, estamos en la obligación de seguir hablando de estas cuestiones y de empujar a nuestras administraciones para que no se rezaguen aún más de lo que ya lo están en esta clase de asuntos. Tal vez es una buena noticia para todos que la Administración no vaya por delante del resto de la sociedad por lo que significa de crecimiento y de maduración de ésta, pero será un mal para todos que la Administración se quede muy atrás. Y en estos asuntos de la sociedad de la información y de la calidad de la cultura democrática, no importa repetirlo, el papel impulsor y ejemplar de la administración es evidente.

3. Referencias

Páginas de Información.

Estados Unidos	
Departamento de Defensa	www.dtic.mil/defenselink/
La Casa Blanca	www.whitehouse.gov/
Estado de Pennsylvania	www.state.pa.us
CNN en español	www.cnnenespanol.com/
The Getty Information Institute	www.ahip.getty.edu/
Librería virtual Amazon	'www.amazon.com/
España	
La Moncloa	www.La-Moncloa.es/
El Senado de España	www.Senado.es/
Congreso de los Diputados	www.congreso.es/
Boletín Oficial del Estado	www.boe.es/
Ministerio de Administraciones Públicas	www.map.es/
Secretaría Gral. de Comunicaciones	www.sgc.mfom.es/
INFO XXI	www.infoxxi.es
Guardia Civil	www.guardiacivil.org/
Otros	
Gov. Information Serv. (CCTA) – UK	www.open.gov.uk/
ISPO (Information Soc. Promotion Office)	www.ispo.cec.be/
Australian Commonwealth Gov.	fed.gov.au/
New Zealand – Government Online	www.govt.nz
Radio B92 OnLine – Belgrado	www.b92.net/
Target Kosovo	www.fas.org/man/dod-101/ops/kosovo.htm
Assoc. for Progressive Communications	*www2.apc.org/english/index.html*
Actuaciones Administrativas.	
"Better Government"	floor.ccta.gov.uk:8080/cogs/cogdisc.nsf
"IT for All"	www.itforall.gov.uk/

Proyecto Infoville (Villena)	www.ovsi.com/infoville
Infoville Móvil	www.infomovil.com/
Proyecto BRAIN (Brent)	brain.brent.gov.uk/
Wales Information Society	www.wis.org.uk/
Participación Democrática.	
"Norwich Connect"	www.norwich.gov.uk/
"21 Aust"	www.link.net.au/21aust/welcome.html
UK Citizens Online Democracy	www.democracy.org.uk/
The Loka Institute	www.loka.org/
Center for Democracy and Technology	ww.icdt.org/
Minnesota e-Democracy	www.e-democracy.org/
Informes	
Reinventing Gov. in the Information Age	www.man.ac.uk/idpm/rgia.htm
Modernising Government White Paper	*www.citu.gov.uk/moderngov.htm*

Green Paper on Public Sector Information in the Information Society
www.echo.lu/info2000/en/publicsector/greenpaper.html

IRISS '98: Conference Papers	osig.ac.uk/iriss/
G7 Government On-line Reports	www.open.gov.uk/govoline/eonline1.htm

Electronic Government - information technologies and the citizen
www.parliament.uk/post/egov.htm

El Delito Informático, Ley 19.223 en Chile, VIII Región, Región del Bío – Bío.

Desafíos al Derecho Informático en el nuevo milenio
Nuevos enfoques de la Informática Jurídica y de los Sistemas aplicados al Derecho en el nuevo milenio

Profesor: Angelo Benvenuto Vera (Chile)
Facultad de Cs. Económicas y Administrativas / Facultad de Cs. Jurídicas y Sociales
Universidad de Concepción - Concepción - Chile

Angelo Benvenuto Vera [1]
Alejandro Rocha N., Miguel Roa G. [2]

1. - RESUMEN

El presente trabajo tiene por objetivo conocer cual es el nivel actual de ocurrencia de delitos informáticos tipificados en la Ley 19223 de fecha 7 de Junio de 1993, en Chile. El universo investigado lo conforma el sector empresarial de la VIII Región-Chile. La muestra fue determinada rigurosamente y sobre esta se aplicó una encuesta especialmente diseñada. El análisis de datos y resultados entrega como conclusión que existe delito informático en el 8.7 % de las empresas encuestadas. Se determinan una serie de indicadores: del tipo, magnitud, y autores, como las áreas que afectan la ocurrencia de delitos. Es posible establecer además, una presencia mínima de controles, y que en general para las empresas, el dato e información, no tiene aún el carácter de bien económico, al evidenciarse la no-provisión de fondos o contratación de seguros, para salvaguardar y proteger este importante activo.

2. - INTRODUCCION, EVOLUCION INFORMATICA EN CHILE

Fue en 1961, cuando la Universidad de Chile dictó sus primeros cursos de Programación de Computadores, un año después, instalaba su primer computador, el "Standard Electronic Lorentz", ER 65. Ese mismo año, la Superintendencia de Aduanas de Valparaíso instaló el primer computador digital comercial del país.

Entre 1962 y 1964 se instalaron unos 20 equipos en Universidades, empresas públicas y privadas. El Banco del Estado de Chile, en los inicios de esta década, instaló el primero de los sistemas de cuenta de ahorro "en línea", conectando sus sucursales a lo largo de todo el país.

En 1975, el número de empresas que incorpora esta tecnología experimentó un aumento explosivo a raíz de la rebaja en los aranceles del 200% al 10%. En la década de los 80 y a partir de 1981, se introdujeron los primeros "Personal Computer" (P.C.) de la I.B.M.

Según cifras proporcionadas por el Banco Central, durante 1987 ingresaron al país 13.762 microcomputadores, lo que estimando a US$ 1.500 la unidad, significaban más de 20 millones de dólares. A raíz de estas estadísticas, y de otras, se ha sostenido que Chile posee el mayor índice de importación de computadores per – cápita de América Latina. Esto ha dado pie a que, en materia de políticas de desarrollo de la Informática, se considere al país, dentro de los que han adoptado una opción decisiva por la difusión y uso de las Tecnologías de Información y Comunicaciones. Un 97 % de las empresas regionales tiene el Sistema Contable automatizado[3].

---

[1] Académico de las Facultades de Ciencias Económicas y Administrativas,. y de Ciencias Jurídicas y Sociales ambas de la Universidad de Concepción – Chile. Departamento de Contabilidad Y Auditoria

[2] Alumnos seminaristas de la Carrera Contador Auditor de la Facultad de Ciencias Económicas y Administrativas de la Universidad de Concepción

[3] A. Benvenuto V. "La Facturación electrónica en la VIII Región – Chile". Ponencia en Conferencia Acad. Permanente de IN. Contable", X CAPIC, Octubre 1999.

La automatización llegó a bancos e instituciones financieras, con lo cual, la transferencia electrónica de datos (sistemas diseñados fundamentalmente para eliminar el flujo de papeles entre bancos y clientes, y para prestar servicios fuera de las oficinas bancarias) se convirtió en una realidad. Actualmente opera la "Sociedad Bancaria de Transferencias Electrónicas S.A., más conocida como Red de Cajeros Automáticos RedBanc.

La integración de Chile a Internet, impulsa a nuevos niveles de desarrollo de la informática en el país. La Bolsa Electrónica de Santiago, afirma que el desarrollo de esta área será explosivo dentro de los tres próximos años, sobre todo en el ámbito del negocio de títulos y acciones. Las proyecciones para las Bolsas Electrónicas de Latinoamérica hablan de un aumento de 7.833 millones de dólares en títulos a negociar en el 2003, con respecto a los 167 millones que actualmente se manejan. "Este súbito desarrollo generará en el sistema un fuerte movimiento en la rotación de acciones y también en la liquidez de los títulos y en la profundidad del mercado"[4]. Existe un nuevo sistema, que permite a los corredores de bolsa recibir órdenes de compra y venta de acciones a través de Internet, y a todos los usuarios desde su hogar u oficinas y simultáneamente, tener acceso a la misma información que los corredores.

Así, en Chile toda entidad privada o gubernamental está trabajando permanentemente en el perfeccionamiento de sus sistemas de información optimizando su gestión y mejorar la rentabilidad del negocios o entidad respectiva. Así por ejemplo una transacción bancaria convencional tiene un costo para el banco del orden de 1.25 dólar, la misma utilizando Internet alcanza a 0.15 centavos de dólar [5]. Ahora bien, parece ser que el resto de las actividades, especialmente aquellas relativas al control, y en general a normar el quehacer del hombre en este ambiente no avanzan a la misma velocidad de incorporación de las Tecnologías de Información y Comunicaciones, de modo de minimizar el riesgo de resultar víctimas de alguna conducta ilícita que atente contra su patrimonio personal, económico u otro.

3. - *EL DELITO EN EL DERECHO CHILENO, ALGUNAS CARACTERISTICAS GENERALES.*

Nuestro Código Penal, a imitación de su modelo español de 1848, y apartándose de la mayor parte de los códigos penales modernos, ofrece una definición de "delito". Ella está contenida en el Art. 1º, inciso 1º, según el cual precisa que, "Es delito toda acción u omisión voluntaria penada por la ley [6]. **Acción u omisión**: Esta expresión es la consagración positiva de dos postulados fundamentales del Derecho Penal Liberal. Por una parte el Principio de Exteriorización: "No puede existir sanción penal si los pensamientos, opiniones o intenciones no se exteriorizan, haciéndose perceptibles", y por otra, el Principio de Legalidad "Una acción es punible sólo si la ley la contempla como tal y la sanciona", "Voluntaria", este término también refleja el pensamiento liberal de que la justificación ética de la sanción penal radica en que el delincuente ha obrado contra la ley a sabiendas y pudiendo haber obrado de otra manera. En otras palabras, esto significa que el delincuente es un ser libre y que ha hecho mal uso de su libertad. Ahora bien, en la medida en que la acción penada es "voluntaria" y "reprochable", es también "culpable". "Ninguna ley podrá establecer penas sin que la conducta que se sanciona esté expresamente descrita en ella". Esto significa que la conducta que se quiere declarar "delictiva" debe necesariamente estar definida en la ley. Y también el de **Antijuricidad; que sig**nifica "contrariedad a Derecho". La "tipicidad" es indispensable, pero no suficiente por sí misma. Es necesario que la ley describa una acción para que ella sea penada; pero además es necesario que la prohiba o la ordene, de modo que quede claro cuándo la acción es "jurídica" y cuándo es "antijurídica".

Ahora bien: sobre la base de todos estos antecedentes doctrinales y legales, es posible definir **"delito"** como: "Toda acción u omisión humana, voluntaria, típica, antijurídica y culpable".

Algunas de las principales características del delito informático son: la permanencia y automaticidad, mayor daño resultante de una sumatoria automática de acciones ilícitas como de permanencia de ocurrencia

---

[4] Entrevista Diario "El Sur" de Concepción a J.C. Spencer, Gerente General de la Bolsa Electrónica de Santiago. (27 de Nov. 1999)

[5] Ejecutivo del "Banco Chile" en entrevista al diario "El Mercurio" de Santiago de Chile, 20 de Agosto de 1999.

[6] Echevrry, A. "Derecho Penal", Tercera Edición, Tomo I, Editorial Jurídica de Chile

en el tiempo, tendencia a crecer en numero de casos y finalmente de difícil detección por la naturaleza del mismo.

La falta de "tipificación", que en la mayoría de las legislaciones presentan los delitos informáticos, es generalmente derivada de lo novedoso que resulta esta materia en relación con la lenta evolución y adaptación a la tecnología informática y comunicaciones que presentan las Ciencias del Derecho.

Tipificación puede definirse como la descripción que hace el legislador de una determinada conducta, estipulándola como **"prohibida"** en una norma legal específica. La ausencia de "tipificación" del delito informático, no sólo puede llevar a la impunidad de ciertos actos claramente ilegales; también deja abierta la posibilidad de excesos y abusos de parte de un Poder Judicial y de una Administración de Justicia que no tenga claridad sobre cuáles conductas debe sancionar y cuáles no.

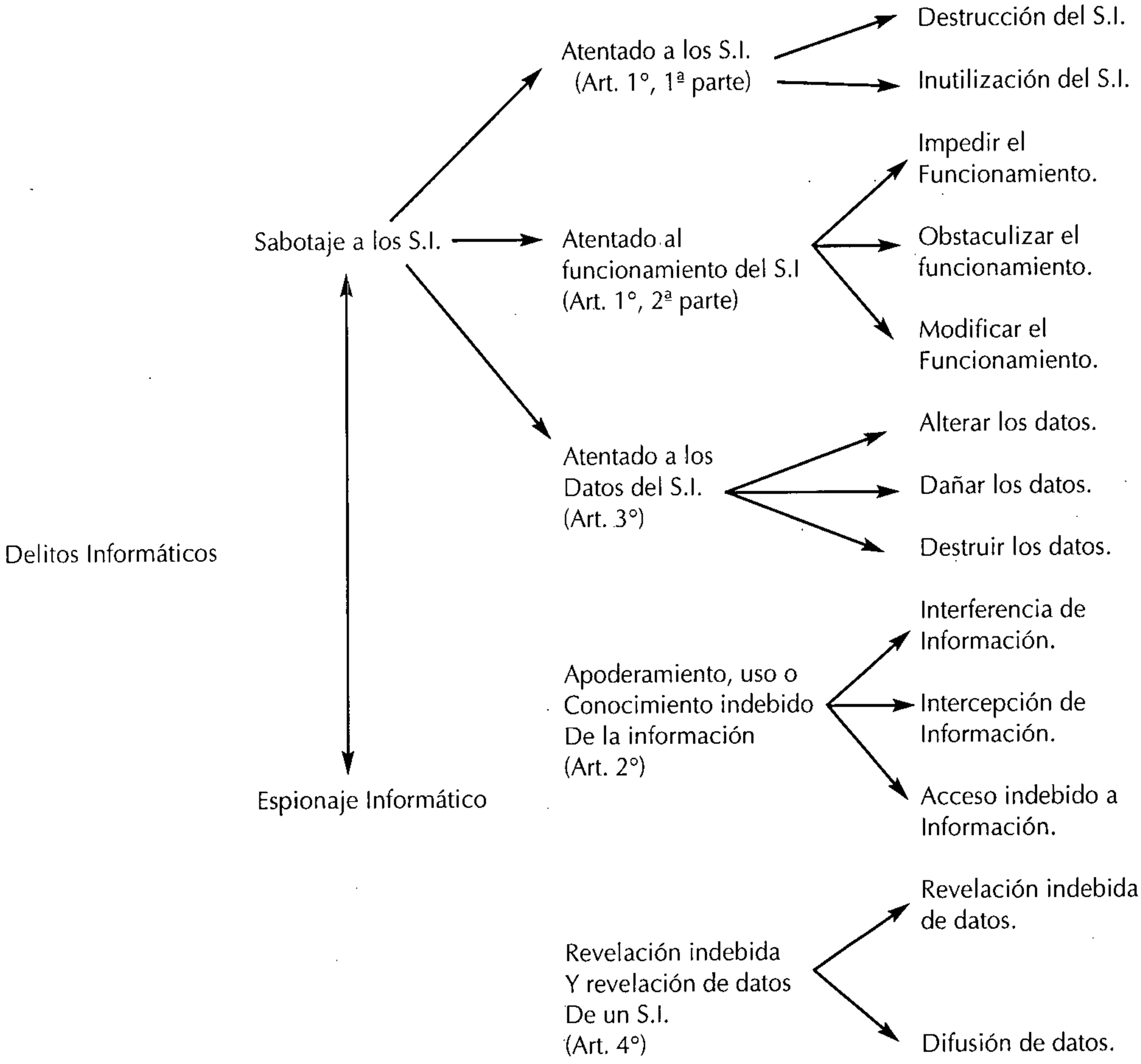
4. - LA LEY 19.223 RELATIVA AL DELITO INFORMATICO. TEXTO COMPLETO EN ANEXO 1.

En lo que se refiere a Chile, la dictación de la Ley N° 19.223 del 7 de Junio de 1993, la cual tipifica figuras penales relativas a la Informática, introduce una novedad de relevancia mundial en cuanto al bien jurídico que es protegido por la tipificación de los Delitos Informáticos. Se trata de la **"Idoneidad y Pureza de las Técnicas de la Informática"**, concepto que permite el tratamiento de estos delitos desde una perspectiva desligada de compromisos y ataduras a las normas tradicionales del Código Penal.

El 16 de julio de 1991, se presentara un proyecto de **"Ley sobre Delito Informático"** a la honorable Cámara de Diputados, que da origen a la primera ley chilena contra el Delito Informático, la Ley N° 19.223. Aún debieron, empero, transcurrir dos años de discusiones teóricas – jurídicas y trámites constitucionales, antes de ser promulgada, el 28 de mayo de 1993, y finalmente publicada el 7 de junio del mismo año en el diario oficial N° 34.584.

La forma en que está propuesta la Ley N° 19.223 tiene antecedentes en la legislación francesa, que data de 1988 y tiene 8 artículos sobre el tema. Esta iniciativa legislativa nacional contiene, no obstante, sólo 4 artículos, referidos exclusivamente a ciertos actos constitutivos de Delito Informático, y no a ideas afines, en virtud de los cuales va ser posible sancionar dichas conductas por las graves consecuencias económicas y sociales que acarrean.

Esquemáticamente se pueden distinguir las figuras penales contempladas en la Ley 19.223:



"Sabotaje Informático", se define como "toda conducta típica, antijurídica y culpable, que atenta contra la integridad de un sistema automatizado de tratamiento de información, de sus partes, de sus componentes, de su funcionamiento o de los datos contenidos en él" [7]

Como puede apreciarse, el sabotaje informático se considera aquí como un acto criminal que puede afectar tanto a los Sistemas de Información propiamente tales, como también a su funcionamiento y a los datos que contienen. Así, el atentado contra el sistema de información, o sus partes componentes, supone un delito que tipifica tanto la destrucción como la Inutilización del sistema de información; el atentado contra el funcionamiento de un sistema de información significa impedir, obstaculizar o modificar este funcionamiento; y, por último, el atentado contra los datos de un sistema de información tiene por punible cualquier acción que altere, dañe, o destruya estos datos. Todas estas conductas ilícitas, se encuentran tipificadas en los artículos 1° y 3° de la mencionada ley.

[7] Huerta M. Marcelo, Líbano M. Claudio, "Delitos Informáticos", Santiago de Chile, Ed. Jurídica Conosur Ltda. 1996.

Por espionaje informático, se entiende "toda conducta típica, antijurídica y culpable, que tiene por finalidad la violación de la reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información" [8]

El espionaje informático se contempla como un delito que incluye, por un lado, el apoderamiento, uso o conocimiento indebido de información ajena o restringida, contenida en un sistema de información, considerándose como conductas punibles típicas la "interferencia", la "intercepción" y el "acceso indebido" a dicha información. Por otra parte, está penalizada también la difusión y la revelación indebida de los datos contenidos en un sistema de información. Estas modalidades de Delito Informáticos se encuentran descritas, respectivamente en los artículos 2° y 4° de la Ley N° 19.223.

Las formas del Delito Informático. Dentro de las prácticas delictuales que han sido circunscritas aquí "propiamente informáticas" (en el sentido en que sólo pueden cometerse mediante el uso del computador, y tienen como objeto jurídico específico a la información), hay que considerar las siguientes:

La Manipulación de Datos, consiste en una "impropia utilización de un sistema de tratamiento de datos, cuyo resultado se traduce en la desviación o alteración de la sana técnica informática, desnaturalizando los datos contenidos en el sistema en cualquiera de las fases de su tratamiento, con o sin ánimo de lucro y en claro perjuicio de terceros". Los actos ilícitos relacionados con "manipulación de datos" en forma individual (alteración de datos, daño de datos, destrucción de datos, etc.). En la Región del Bío-Bío, no se ha conocido hasta la fecha proceso alguno relativo a denuncias por conceptos y delitos contemplados en la Ley 19.223.

5. - EL ESTUDIO EN LA VIII REGION, REGION DEL BIO-BIO.

5.1 Del Marco Teórico de la Investigación.

Lo desarrollado precedentemente constituye un marco referencial jurídico general que enmarca el presente trabajo. En este capítulo se expondrá la planificación, la ejecución y los resultados del estudio, cuyo objetivo general es determinar la incidencia del Delito Informático en las empresas de la región. La delimitación precisa de este estudio requiere que previamente se analice una serie de aspectos, tanto teóricos, prácticos y estadísticos.

En relación con aspectos teóricos la investigación corresponde a un estudio pionero, no existen estudios relativos a Delito Informático en las Empresas. Se estima que la forma más apropiada de recopilar información general por primera vez es mediante la aplicación de una encuesta. Tratándose de un tema tan delicado como es el Delito Informático, cuya ocurrencia puede acarrear serios daños económicos como a la imagen de la empresa, es previsible que, parte de los datos declarados por los sujetos entrevistados no sean fidedignos, o que, simplemente, no se responda la encuesta. No existe otra alternativa de sondear, tanto o más directa que la encuesta, y que pueda eludir el silencio o la tergiversación de la información aportada por los consultados.

5.2 Respecto de los alcances estadísticos se debe señalar que el universo de empresas a encuestar esta delimitado por los criterios siguientes:

Que estas empresas cuenten con algún grado de automatización de sus sistemas de información operacional, financiera y de gestión. Las señales que pueden confirmar esta característica en una empresa son Empresas con correo electrónico y página Web en guías clasificadas y publicidad televisiva o de diarios, con más de una sucursal en la publicidad de guías clasificadas y de diarios, que la actividad o giro de estas empresas suponga la administración de activos líquidos de otras personas naturales o jurídicas y la administración de información de otras personas naturales o jurídicas. Finalmente el método a emplear será el Método de Muestreo Estratificado, y el criterio de estratificación adoptado será el giro o sector de actividad economía al cual pertenece la empresa.

---

[8] Id.

5.3 De La Formulación de Hipótesis

El procedimiento planificado y ejecutado según se establece a continuación tiene como finalidad la comprobación de 3 hipótesis claves, que se sostienen sobre la base de los antecedentes bibliográficos revisados y analizados precedentemente.

El Delito Informático existe en un determinado porcentaje de empresas de la Región".

El Delito Informático, cuando es perpetrado, afecta gravemente el desenvolvimiento de las empresas.

Las empresas pueden establecer controles y medidas de seguridad lo suficientemente eficientes como para poder prevenirse contra el Delito Informático.

El dato es considerado como un recurso corporativo con características de bien económico que esta expuestos a riegos debiendo existir provisiones económicas para su seguridad, respaldo e integridad

5.4 De la Metodología y determinación de la muestra piloto y muestra definitiva. La metodología aplicada para el análisis de los datos corresponde a un método de muestreo probabilístico, ya que este permite evaluar la precisión de las estimaciones, el cómputo de estadígrafos, medir el error de muestreo y estimar cuantitativamente los parámetros a partir de estadígrafos.

El elemento poblacional queda definido como e l conjunto de empresas medianas y grandes según el criterio de números de trabajadores de los sectores económicos más relevantes de la Octava Región". Los sectores industriales más relevantes en la Octava Región son el sector comercial-industrial, pesquero, forestal, educacional, financiero, servicios.

Tabla 5.1 Empresas VIII Región según sector industrial

Sector	Com.-Ind.	Forestal	Pesquero	Educación	Financiero	Servicio	Total
Nº Empr.	224	35	40	66	22	95	482

Se define el universo de empresas a considerar, "N", para la determinación de la "muestra" o número total de empresas a encuestar. Las empresas que compondrán la cifra "N" deberán extraerse de bases de datos especializadas, guías clasificadas, spots publicitarios de televisión, publicidad gráfica de diarios y revistas, etc., siguiendo los criterios de selección definidos.

La determinación del número de empresas de la muestra "n" requiere introducir en la fórmula un parámetro "p_" por cada sector "j" (j= 1, 2, 3, 4, 5, 6). Este parámetro representa **la proporción de Delitos Informáticos acaecidos según antecedentes pasados**. Como tales antecedentes no existen, la metodología estadística aconseja efectuar una **muestra piloto**. Se acuerda considerar como "muestra piloto", el 10% del universo de empresas de cada sector "N_". Este 10% es la cantidad para cada estrato, "n_ m.p.". Cada "hallazgo" de un Delito Informático en un sector "_" se simboliza "A_".

Se planifica aplicar la encuesta contactando a las empresas de tres modos; vía correo electrónico, por teléfono, vía entrevista personal. En cada contacto se procurará que el entrevistado sea el encargado del **Departamento de Informática de la Empresa**, o un empleado o funcionario que esté informado de todos los aspectos que se consultarán.

El "Muestreo Piloto" del 10% de las empresas de cada estrato arrojó "A_"= 3 hallazgos, 1 en el Sector Comercial – Industrial y 2 en el sector Educacional. Sobre la base de este dato empírico, los parámetros "p_"

dieron, para el sector Comercial - Industrial un p1= 0,04545; y para el sector Educacional un p4= 0,28571.

Y, en consecuencia, la resolución de la fórmula para el "muestreo estratificado", indica que la muestra mínima de empresas a encuestar, para un error estimado de E= 0,05 y un nivel de confianza de 95%, es n= 65 empresas.

p_= Aj/nj m.p. (m.p., muestra piloto)

A_= Hallazgos de Delito Informático.

n_ m.p.= 10% de Nj.

N_= Total de empresas por cada estrato _.

p_ = Proporción del Delito Informático.

$$E = Z_{1-/2} \times \frac{1}{N} \sqrt{\left(\frac{N}{n} - 1\right) \times p^{o} \times q^{o} \times \frac{N^{o}_{-}}{N^{o} - 1}}$$

$$N^{o} = \left(\frac{n}{N}\right) \times N^{o}$$

E= Error en la determinación de la existencia del Delito Informático.
Z 1-/2 = Nivel de Confianza.
$q^{o} = 1 - p^{o}$= proporción de no-ocurrencia del Delito Informático.

Tabla 5.2 Hallazgos de eventos en Muestra Piloto según sector actividad económica

	N_	n_(M. Piloto)	A_	p_
Com.-Industrial	224	22	1	0.0454
Forestal	35	4	0	0
Pesquero	40	4	0	0
Educacional	66	7	2	0.2857
Financiero	22	2	0	0
Servicios	95	10	0	0
Total	**482**	**49**	**3**	

6. - PRESENTACION Y ANALISIS DE LOS DATOS

Se presenta a continuación en una serie de Tablas los datos debidamente ordenados, clasificados y procesados. Las tablas presentan los distintos tipos de indicadores porcentuales obtenidos después de los cálculos correspondientes. Los principales indicadores son: Porcentaje de delitos en las empresas según sector o actividad económica, tipos de delitos y formas de manipulación de los equipos, autorías del delito, nivel dentro de la organización y forma de detección, perdidas estimadas por año, duración de la conducta delictiva y área funcional de la empresa afectada, finalmente se presentan las medidas de respaldo económico o computacional, tanto en el total de las empresas como en aquellas empresas víctimas del delito.

Tabla 6.1 Hallazgos de eventos en Muestra Definitiva según sector actividad económica

Sector	N_	P_	n_	U *	A_	% Delito sobre (U)
Com/Ind	224	0,0454	30	31	1	**3.3**
Forestal	35	0,0000	5	5	0	**0**
Pesquero	40	0,0000	5	5	0	**0**
Educacional	66	0,2857	9	9	3	**33.3**
Financiero	22	0,0000	3	6	1	**16.6**
Servicios	95	0,0000	13	13	1	**7.69**
Totales	482		65	69	6	**8.70**

*** U = Número total de encuestas aplicadas**

De los datos de la tabla se observa que el sector económico mas afectado por la ocurrencia de situaciones delictivas es el Educacional, seguido por los sectores Financiero, Servicios y Comercial e Industrial respectivamente, los sectores Pesca y Forestal no presentan ocurrencias.

Tabla 6.2 Tipo de delito y forma de manipulación del computador

Tipo de Delito	%	Manipulación	%
Accesos indebidos	22.2	Modifica Programas Fte.	28.55
Modifica Funcionamiento	22.2	Modifica Datos entrada	14.30
Modifica datos	11.1	Ingreso no autorizado	14.30
Destrucción de datos	11.1	Modifica datos salida	14.30
Uso indebido de datos	33.4	Omite datos de E/S	28.55
	100		100

El cuadro precedente evidencia sin mayores explicaciones cuales son los tipos de conductas delictivas y la acción específica de manipulación que se efectúa. Los tipos corresponden globalmente a 44.4 % de delitos que afectan al Sistema de Información en lo que a funcionamiento se refiere, y un 55.6 % están relacionados con el contenido de los archivos de datos del Sistema. En lo referido al tipo de manipulación, un 42.85 % corresponde a la parte operativa, (modificación de programas más accesos indebidos), y un 57.15 % se manipulan los datos.

Tabla 6.3 De los autores, Nº de personas, su nivel jerárquico dentro de la empresa y forma de detección del delito

Nº de pers.	%	Nivel	%	Detección	%
1	66.6	Gerencial	0	Fortuita	33.3
2 (1 /1) *	16.6	Administrativo	14.3	C. Auditoria	33.3
Indeterminado	16.6	Operativo	71.4	Infraganti	16.6
		Indeterminado	14.3	Entrevistas	16.6
	100		100		100

* Esto corresponde a una persona de la empresa coludida con una persona externa a la empresa.

Puede apreciarse en el contenido de la tabla, que el autor de un delito, actúa normalmente solo, o asociado a una persona más, un alto porcentaje de los autores pertenece a niveles operativos. Llama la atención que un significativo porcentaje (46.9 %) es detectado no por consecuencia de controles y auditorias en las empresas o infraganti.

Tabla 6.4 Del Delito, Área que afectó a la empresa, la pérdida ocasionada / año y la duración del delito

Pérdidas	%	Área	%	Duración	%
< 2000 $USS	50	Operaciones	48.9	3 años	16.66
> 2000 $ USS	33.3	Finanzas	48.9	1 año	16.66
Indeterminada	16.7	Otra	14.2	2 a 6 meses	50.00
				Incalculable	16.66
	100		100		100

Parece ser, que la cuantía de los daños económicos no es significativa al menos en forma cuantificable, oportuno es señalar del 16.66 % que ha señalado como incalculable las pérdidas ocasionadas, casi un 50 % de las áreas afectadas son las relativas a la Contabilidad y Finanzas de una empresa. En el tipo de otras áreas, estas dicen relación con calificaciones o notas de establecimientos educacionales.

Tabla 6.5 De las medidas de respaldo económico ante posibles ocurrencias de un D. Informático, total empresas y en aquellas afectadas por D. Informáticos.

En el total de las Empresas:		En empresas con Delito Informático:	
Medidas	**%**	**Medidas**	**&**
Ninguna	18.8	Ninguna	33.3
No sabe, no contesta	72.5	No sabe no contesta	66.7
Respaldos Físicos	2.9		
Seguros	2.9		
Provisión de Fondos	2.9		
Total	**100**		**100**

La información contenida en este cuadro, estaba dentro de lo previsible, confirmada ahora, en general las empresas no toman medidas para cautelar los datos e información, o bien, si ha tomado medidas estas no son conocidas o no son dadas a conocer. Coinciden los valores más altos en empresas con ocurrencia de delitos como en aquellas que no han sido víctimas. El porcentaje mas alto corresponde a la respuesta "No sabe, no contesta", se puede deducir que el desconocer las medidas correspondería teóricamente a que estas no existen.

7. - CONCLUSIONES

El Delito Informático existe en el contexto empresarial de la VIII Región, Región del Bío-Bío. El presente estudio señala que un 8,2% de las empresas regionales han sido víctimas de la menos un delito. Por sectores de actividad económica los porcentajes son los siguientes: 3,2% para el sector Comercial – Industrial, 33,3% para el sector Educacional, en un 16.6 % para el sector Financiero y en un 7,69 % para el sector Servicios. Ni el sector Forestal ni el sector Pesquero acusaron ocurrencia alguna de este tipo de delito. El sector Educacional fue el que tuvo la más alta tasa de sucesos informáticos delictivos, lo cual puede tener su explicación en que son las instituciones que menos resguardo ponen a su información automatizada. En el caso de los departa-

mentos de computación de institutos y colegios, no existen motivos para proteger, a costos relativamente elevados, datos sobre notas, antecedentes escolares.

Existe, definitivamente, una correlación inversa entre la existencia de controles, resguardos, respaldos y provisiones, con la ocurrencia del Delito Informático. El sector empresarial, en un altísimo porcentaje general no tiene medidas de respaldo financiero o contratación de seguros para cautelar este nuevo patrimonio que es el dato e información. Probablemente la carencia de una metodología universalmente aceptada para cuantificar económicamente este recurso, impide a las empresas determinar el "que" y "cuánto" invertir, en aspectos de control, seguridad y auditoría. El dato e información ha adquirido el carácter de objeto jurídico a proteger, convirtiéndose en un bien económico más, recurso indispensable en el contexto actual, en que la sociedad globalizada toda, es soportada por economías basadas en el conocimiento e información.

BIBLIOGRAFIA

Acha Iturmendi, J. José: **"Auditoría Informática en la Empresa"**, Madrid, Editorial Paraninfo, 1994, 177 páginas.

Chateau, Jorge: **"Manual para la Elaboración de Cuestionarios y Pautas de Entrevistas"**, 2da edición, Santiago, Editorial Flacso, diciembre de 1991, 74 páginas.

Garrido Montt, Mario: **"Nociones Fundamentales de la Teoría del Delito"**, Santiago, Editorial Jurídica de Chile, 1992, 192 páginas.

Guerrero Mateus, María Fernanda & Santos Mora, Jaime: **"Fraude Informático en la Banca: Aspectos Criminológicos"**, Ediciones Lesma, 1993, 124 páginas.

Huerta Miranda, Marcelo & Líbano M., Claudio: **"Delitos Informáticos"**, Santiago, Editorial Jurídica Conosur Ltda., 1996, 377 páginas.

Jijena Leiva, Renato: **"Chile, la Protección Penal de la Intimidad y el Delito Informático: ¿Un problema de Tipificación?. Análisis del Proyecto Chileno de Legislación"**, Valparaíso, Escuela de Derecho, Universidad Católica de Valparaíso, 1990, 202 páginas.

Mir Puig, Santiago: **"Delincuencia Informática"**, 1ª edición, Barcelona, P.P.V. (Promociones y Publicaciones Universitarias), 1992, 182 páginas.

Tausanes, Ramón y Gallego Santiago: **"Diccionario de Economía y Finanzas"**, Madrid, Alianza Editorial, 1994, 925 páginas.

Suplemento **Siglo XXI**, ***El Mercurio***, 3 de noviembre de 1994.

Diario **El Sur**, 27 de noviembre de 1999.

Echeverry, A.: **"Derecho Penal"**, 3ª Edición, Tomo I, Editorial Jurídica de Chile, 361 páginas.

Boletín Oficial Nº 412 – 07, de la Honorable Cámara de Diputados y Senado de Chile.

Muxica H., Luis: **"Probabilidad, Distribuciones de Probabilidad y la Teoría del Muestreo"**, Concepción, Escuela de Economía y Administración, Universidad de Concepción, 1963, 213 páginas.

ANEXOS

Anexo 1: Ley Relativa a Delitos Informáticos

Artículo 1º. - *El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus* partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º. - El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º. - El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º. - El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

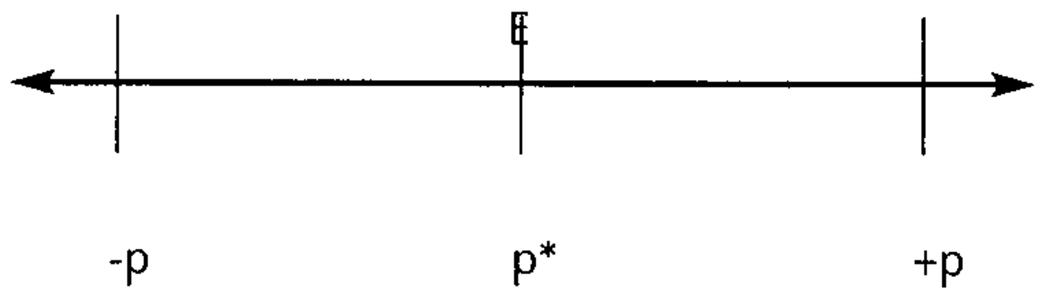
Santiago, 28 de Mayo de 1993. - ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia.

Lo que transcribo a Ud. para su conocimiento.-
Saluda atentamente a Ud., Martita Worner Tapia, Subsecretario de Justicia.
Identificación de la Norma: LEY-19223
Fecha de Publicación: 07.06.1993
Fecha de Promulgación: 28.05.1993
Organismo: M Justicia.

Anexo 2: Cálculo del número de empresas de la muestra mínima para un "Muestreo Aleatorio Estratificado"

El error en la determinación de la existencia de "delito informático, "E", se define por la diferencia absoluta entre la proporción real del Delito Informático, "p*", y la proporción estimada "p". Se desea que no resulte superior a un 5%.

E= | p* - p | = 0,05



Considerando que la muestra "n" sea suficientemente grande (n>30), por aplicación del "Teorema del Límite Central", se puede afirmar que la misma diferencia absoluta tiene distribución normal, con media 0 y varianza "p x q"= 1.

| p* - p | ~ N(0, pq)

de modo que se puede exigir para esta muestra un intervalo de confianza basado en los valores de la función de Distribución Normal Estándar (z)= P(Z z).

Así, si exigimos un nivel de confianza del 95% para esta muestra:

1 - = 0,95
= 0,05
/2= 0,025
1 - /2= 0,975

Según la tabla para los valores de la Distribución Normal Standard:

Z (1 - /2)= Z (0,975)= 1,96

$$E = Z(1-/2) \times \frac{1}{N} \sqrt{\left(\frac{N}{n} - 1\right) \times p^{o} \times q^{o} \times \frac{N}{N^{o} - 1}}$$

$$0{,}05 = 1{,}96 \times \frac{1}{482} \sqrt{\left(\frac{482}{n} - 1\right) \times 23{,}43955}$$

$$(12{,}29592)_ = (482/n - 1) \times 23{,}43955$$

$$7{,}45019 = 482/n$$

$$n = 65$$

$$n^{o} = (n/N) \times N^{o}$$

$$n^{o} = (65/482) \times 482$$

$$n^{o} = (0{,}13485) \times N^{o}$$

Anexo 3: Encuesta

Sr. Entrevistado (a):

El presente cuestionario forma parte de una investigación del Prof. Angelo Benvenuto V. Relativo al Delito Informático en las empresas de la región, colaboradores de son los alumnos Srs. A. Rocha N. Y M. Roa. G. seminaristas de la **Universidad de Concepción**, se cuenta con la colaboración de académicos de las más variadas disciplinas pertenecientes a la facultad de Ciencias Económicas y Administrativas, Facultad de Ciencias Jurídicas y Sociales y de la facultad de Ciencias Físicas y Matemáticas.

Se trata del primer intento por establecer el grado de ocurrencia del **Delito Informático** en empresas de la provincia de Concepción.

Por medio de este instrumento, se procura reunir la información necesaria para establecer, sobre bases fidedignas, **cómo afecta a las empresas** esta nueva forma de **delito**, que tiene por eje el creciente **uso de la computación** y la ***informática***, y ***de qué manera pueden las empresas prevenirse razonablemente***.

El cuestionario consta de 12 preguntas, elaboradas en términos muy generales pero precisos. No se requiere de ningún tipo de identificación, con el objeto de **garantizar la absoluta confidencialidad** de la información proporcionada.

En cualquier caso, el único valor que tiene esta información es **Estadístico**. Por lo mismo, se solicita que las respuestas sean lo más honestas y veraces que se pueda. Sólo así podremos reflejar la auténtica **vulnerabilidad de las empresas**. Y, sobre la base de este diagnóstico, nos será muy grato el compartir con ustedes conclusiones válidas, para que **puedan afrontar la amenaza creciente del Delito Informático** de una manera debidamente fundamentada y eficaz.

Abreviaturas utilizadas: **D.I. : Delito Informático** **S.I. : Sistema de Información**

PREGUNTAS

1.a) ¿Ha habido algún caso de D.I. en esta Empresa?

1.- ..... SI 2.- ..... NO

1.b) ¿Cuántos casos? .....

1.c) ¿Qué tipo de D.I. se cometió en cada caso?

1.- ..... Inutilización de un S.I.
2.- ..... Modificación del funcionamiento de un S.I.
3.- ..... Intercepción de un S.I.
4.- ..... Interferencia de un S.I.
5.- ..... Acceso indebido a un S.I.
6.- ..... Alteración de los datos de un S.I.
7.- ..... Destrucción de los datos de un S.I.
8.- ..... Revelación de los datos de un S.I.
9.- ..... Difusión de los datos de un S.I.
10.- ..... Otro: .....

2. ¿En qué forma se MANIPULO el computador para llevar a cabo el D.I.?

1.- ..... Ingreso no autorizado al S.I.
2.- ..... Modificación de programas fuertes
3.- ..... Alteración de registros magnéticos.
4.- ..... Modificación de datos de entrada.
5.- ..... Modificación de datos de salida.
6.- ..... Omisión de datos de entrada.
7.- ..... Omisión de datos de salida.
8.- ..... Otro: .....

3. ¿En cuánto se estiman las pérdidas sufridas por la empresa a raíz del D.I.?

1.- ..... miles de pesos (sólo si la estimación es INFERIOR a 1 millón)
2.- ..... millones de pesos

4. ¿A qué área de la empresa afectó el D.I.?

1.- ..... Operaciones 2.- ..... Marketing/Ventas
3.- ..... Contabilidad 4.- ..... Finanzas
5.- ..... Otra: .....

5. ¿Cuántas personas estuvieron involucradas en el D.I.? .....

6. ¿Cuántos de los involucrados en el D.I. pertenecían a la empresa? .....

7. ¿Qué posición ocupaban los involucrados en la empresa?

1.- ..... Nivel gerencial
2.- ..... Nivel administrativo
3.- ..... Nivel operativo

8. ¿Durante cuánto tiempo se perpetró el D.I.?

1.- ..... meses 2.- ..... años

9. ¿En qué forma fue descubierto el D.I.?

.....
.....

10. ¿Qué medidas de control existen actualmente en esta empresa para la prevención y detección de posibles D.I.?

    1. ..... Supervisión de las tareas que ejecuta el usuario.
    2. ..... Controles de acceso a información (códigos de usuario, password, etc.)
    3. ..... Auditorías informáticas periódicas.
    4. ..... Políticas de prevención del D.I.
    5. ..... Otro: .....

11. ¿Qué medidas de Respaldo Económico mantiene la Empresa ante la posible ocurrencia de un D:I.?

    1. ..... Contratación de un "Seguro contra pérdidas por D.I."
    2. ..... Mantención de un "Fondo" o "Provisión" para cubrir eventuales pérdidas por un D.I.
    3. ..... Otra: .....

12. ¿ Cómo CLASIFICARIA esta Empresa?

    12.a) Según su TIPO:

    1. ..... Pública.
    2. ..... Semifiscal.
    3..... Privada.

    12.b) Según su GIRO:

    1. ..... Comercial.
    2. ..... Industrial.
    3. ..... Financiera.
    4. ..... Forestal.
    5. ..... Agrícola.
    6. ..... Pesquera.
    7. ..... Otra: .....

Conflictos de Leyes y de Jurisdicción en el Cyberespacio: Una tesis de trabajo desde la perspectiva del Derecho Internacional Privado Español

Marina Vargas Gómez-Urrutia[1] (España)
Profesora Asociada de
Derecho Internacional Privado
Universidad Nacional de Educación a Distancia (España)

Del 24 al 29 de Abril 2000

RESUMEN

El Derecho internacional privado no es ajeno a las cuestiones que plantea el uso de medios tecnológicos nuevos, como es Internet, para llevar a cabo transacciones jurídicas de tráfico privado externo. De ahí que quepa interrogarse sobre si sus técnicas de reglamentación y las soluciones que el derecho interno ofrece en los sectores de ley aplicable y de competencia judicial, son aptas para resolver los supuestos de tráfico jurídico externo que se producen de forma desmaterializada en este espacio sin fronteras. En esta comunicación se abordan algunas cuestiones relacionadas con los conflictos de leyes y de jurisdicciones que pueden darse en las transacciones transnacionales y en otras actividades comerciales que se desarrollan en la Red, todo ello desde la óptica del Derecho internacional privado español.

INTRODUCCION

El verdadero "mascarón de proa" de los problemas jurídicos que plantea la sociedad de la información se encuentra en la utilización creciente de una red abierta, como es *Internet,* que permite la edición y distribución masiva, y en línea, de informaciones de toda índole. Desde la óptica del DIPr. las preguntas han de ir necesariamente vinculadas a la determinación de los derechos de los particulares y a los modos de protección de los mismos. La técnica que sigue cada país o cada legislación va a provocar necesariamente una respuesta distinta de cara al tráfico externo, planteándose entonces disyuntivas en torno a la competencia judicial internacional y a la ley aplicable.

La objeción de que las soluciones jurídicas de derecho interno carecen de viabilidad para regular las relaciones jurídicas que se conciertan por vía de *Internet,* o para regir la propia Red de Redes, puede ser despejada, *prima facie,* partiendo de una afirmación que no merece mayor demostración: **es perfectamente normal que situaciones jurídicas conectadas con varios ordenamientos extranjeros sean sometidas al Derecho de uno o de varios Estados.**

Las dificultades para la determinación de este Derecho, cuando son varios los elementos de internacionalidad que aparecen en el supuesto de hecho, son bien conocidas por los especialistas de DIPr[2].

Lo anterior nos lleva a afirmar como tesis de trabajo que ***Internet,* lejos de ser un espacio virtual desgajado de cualquier ordenamiento jurídico nacional, es un sistema de redes interconectadas que une millares de ordenadores del mundo entero. Aquí se prestan servicios de información y de comunicación entre usuarios,**

---

[1] Profesora Asociada de Derecho internacional privado. Universidad Nacional de Educación a Distancia. Madrid (España).

[2] Debe señalarse que como el objeto de este trabajo está focalizado en algunos aspectos relacionados con el comercio electrónico e Internet, no trataremos los aspectos doctrinales generales de DIPr., cuya bibliografía es abundantísima y excedería con mucho de la finalidad de este estudio.

sujetos que desarrollan actividades muy diversas, las cuales habrán de ser reguladas bien mediante leyes materiales o sustantivas, o bien mediante normas conflictuales de Derecho internacional privado

Se pueden proponer alternativas tales como la elaboración de leyes modelo que partan de las peculiaridades de la Red; o bien, la adaptación de reglas ya existentes para otros medios de comunicación ya conocídos y surgidos de los avances de la tecnología (sector de radio y televisión, por ejemplo). Por ello, toda propuesta que parta de la elaboración de una supuesta *International Cyberlaw* no puede hacer abstracción de las leyes ya en vigor, sean materiales o conflictuales, que se aplican a situaciones jurídicas transnacionales similares[3].

En esta comunicación vamos a abordar algunas cuestiones que afectan al comercio electrónico desde la óptica del Derecho internacional privado. El punto de partida, como se ha dicho antes, es evaluar la pertinencia de las normas existentes en materia de conflicto de leyes y de competencia judicial internacional (conflictos de jurisdicción) en el Derecho internacional privado español con el fin de saber si sus soluciones son o no viables y aptas en este nuevo "espacio" virtual.

I. LA MATERIA CONTRACTUAL Y EL COMERCIO ELECTRONICO

Como primera provisión cabe señalar que los contratos informáticos son particulares, más no por el tipo contractual. Los tipos empleados son los de siempre, es decir responden a la arquitectura tradicional de contratos ampliamente conocidos: compraventa, *leasing*, arrendamiento, arrendamiento de servicios, etc. Su particularismo, como ha puesto de relieve la doctrina[4], radica en otros factores: de un lado, por el objeto de tales contratos, frecuentemente constituido por bienes incorporales (*ad.ex.* contratos de *Hardware-Software*, contratos de desarrollo de *Software*, contratos de concesión comercial de *Software*, contratos de tratamiento de datos, contratos de utilización de datos, contratos de recursos informáticos o, contratos de estrategia informática); y, de otro, porque aparecen coaligados a otros contratos relacionados entre sí por su objeto, así como porque, en ocasiones, implican la afectación de la intimidad de los individuos (*privacy*), sobre todo en los contratos sobre tratamiento de datos (EDP).

Unido a esto, la internacionalización de los medios de transmisión de la información y la apertura de mercados nacionales, hacen que estos contratos presenten con frecuencia un carácter internacional (*ad.ex.* licencia internacional de uso de *Software*, o *leasing* internacional de equipo informático, o un contrato internacional de transferencia de datos informatizados). Este carácter suele derivar del hecho de que los contratantes tienen su sede en diferentes países, más no de la circunstancia de que en las fases de la negociación, o en alguna de las transacciones llevadas a cabo, se haya utilizado el medio técnico de la electrónica o el instrumento de comunicación de *Internet*.

Para saber qué ley aplicar y qué tribunal tendrá competencia para conocer de un contrato internacional **NO efectuado en línea**, las reglas actuales de DIPr. español están contenidas en los siguientes cuerpos normativos[5]: **a) normas sobre competencia judicial**: *Convenio relativo a la competencia judicial a la ejecución de re-*

---

[3] La Conferencia de La Haya de Derecho Internacional Privado en Mesa Redonda llevada a cabo en Ginebra a finales del pasado mes de septiembre, ha planteado las cuestiones sobre la competencia judicial internacional y la ley aplicable derivadas del comercio electrónico y de las operaciones efectuadas por medio o a través de Internet. Las conclusiones pueden ser consultadas en la página web de la propia Conferencia o bien en el sitio <http://cuiwww.unige.ch/billard/ipilec>.

[4] Carrascosa González, J., "Contratos en el sector audiovisual e informático", en Contratos Internacionales, (A.L. Calvo Caravaca y L. Fernández de la Gándara, Dir), Tecnos, Madrid, 1997, p. 1711; Mankowski, P., "Das Internet im InternationalenVertrags- und Deliktrecht", *RabelsZ BD. 63 (1999), pp. 231-256.*

[5] Advertencia: En materia de obligaciones existen en nuestro DIPr. de producción interna normas de derecho civil, mercantil y laboral de carácter especial que regulan la materia en sectores específicos del ordenamiento (ad. ex. seguros, condiciones generales de la contratación, defensa de consumidores, títulos valores y ordenación del mercado). Lo mismo sucede en el DIPr. de origen convencional en donde existen convenios de ámbito material especial, ad.ex., sobre ley aplicable a la materia de accidentes de circulación por carretera o ley aplicable a la responsabilidad por productos, entre otros. En esta exposición sólo nos referiremos a las normas generales.

soluciones judiciales en materia civil y mercantil y Protocolo anejo, hechos en Bruselas el 27 de septiembre de 1968 *DOCE* núm. C 189, de 28 de julio de 1990 y versión consolidada (*DOCE* núm. 27, de 26 de enero de 1998); y Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano el 16 de septiembre de 1988 (*BOE* 251, de 20 de octubre de 1994; corr. errores BOE, 8 de 10 de enero de 1995); **b) normas sobre ley aplicable**: *Convenio sobre la ley aplicable a las obligaciones contractuales*, hecho en Roma, el 19 de junio de 1980 (BOE, 171, de 19 de julio de 1993, corr. errores, *BOE* 189, de 9 de agosto de 1993); *Convención de las Naciones Unidas sobre los contratos de compraventa internacional de mercaderías*, hecha en Viena el 11 de abril de 1980 (BOE, 26 de 30 de enero de 1991; corr. errores BOE 282, de 22 de noviembre de 1996). Y, en el derecho de producción interna, habrá que acudir, cuando resulten de aplicación al art.22.3 de la Ley Orgánica del Poder Judicial (para la determinación de la competencia judicial internacional de los tribunales españoles) y al artículo 10.5 del C. civil (con carácter residual, para la ley aplicable).

En cuanto a la determinación del tribunal competente. La primera dificultad que se presenta es la de establecer **"el lugar de ejecución de la obligación que sirve de base a la demanda"**. ¿Cómo se fija este lugar en un contrato *on line*? Como primera aproximación cabe distinguir entre operaciones electrónicas únicamente entre profesionales y operaciones electrónicas entre profesionales y consumidores, ya que los intereses en presencia y la protección que se dispensa al consumidor en este tipo de contratos aconsejan buscar soluciones distintas. Dadas las dificultades para establecer con precisión el lugar de ejecución de un contrato *on line*, algunos autores consideran que este factor de conexión no resulta apropiado para las transacciones comerciales que se realizan en un ambiente electrónico, por lo que se ha propuesto fijar como factor de localización el del lugar de "**situación**" de una de las partes.

El anteproyecto de Convenio de la Conferencia de La Haya de DIPr., sobre la competencia y la ejecución de sentencias extranjeras en materia civil y mercantil (adoptada por la Comisión el 30 de octubre de 1999) recoge en su artículo 4 la posibilidad de elección de foro mediante cláusulas concluidas o confirmadas "por cualquier medio de comunicación que permita acceder a la información y ser consultada ulteriormente", en clara referencia a los contratos concertados por medios electrónicos.

Pero, ¿será esta la mejor solución cuando nos encontramos en el marco del comercio electrónico entre consumidores? A primera vista podría afirmarse que las cuestiones y los problemas jurídicos que se presentan y afrontan en un "ambiente electrónico" no tienen en sí mismos considerados un carácter novedoso; ya hemos dicho que los contratos que se concluyen en la red son tipológicamente iguales que cualquier otro contrato. Por ende, no tendría que haber mayor problema para proteger al consumidor siguiendo la normativa existente para los contratos de consumo. Pero no conviene quedarse en este punto, lo que lo que merece la pena destacar de esta nueva realidad es la **"escala y la dimensión internacional" circunstancia que provoca que el número de operadores del comercio electrónico y las transacciones comerciales concertadas electrónicamente crezcan de modo exponencial**. Esta característica es la que merece retenerse en aras al establecimiento de "nuevas estrategias legislativas" que protejan de modo adecuado y eficaz a usuarios, consumidores, y sobre todo los valores fundamentales del ordenamiento jurídico.

Para la determinación de la ley aplicable, en ausencia de elección, la regla que sirve de base es el art.4 CR que señala que el contrato se regirá por la **ley del país con el que presente los vínculos más estrechos**, permitiendo el *depeçage* si una parte del contrato fuera separable del resto y presentara una vinculación más estrecha con otro país. Para fijar o precisar "los vínculos más estrechos" el art. 4.2 del CR presume que es **el país en que la parte que deba realizar la prestación característica tenga en el momento de celebración del contrato, su residencia habitual**.

Cuando estamos en presencia de un **contrato *"on line"***, la determinación del derecho aplicable, en ausencia de elección, obliga a precisar **la ley de la sede del prestador característico**. Como hemos dicho anteriormente, los contratos *on line* no se distinguen tipológicamente hablando de los contratos no formalizados *"en línea"*, por lo que las dificultades para la precisión del derecho aplicable son idénticas a las que se presentan en el resto de los contratos. Debe recordarse, no obstante, que en muchos de los contratos que se concier-

tan en la Red la cláusula sobre elección de ley suele venir preestablecida. Piénsese por ejemplo en un contrato de licencia de uso de Software. Aquí la licencia de uso suele venir en el "contenedor externo del programa" (el CDROM o *kit* de instalación), adhiriéndose el adquirente-licenciatario a las condiciones contractuales de la licencia con el mero hecho de abrir el programa "*cliqueando*"[6] en el icono de "aceptar" (son licencias conocidas como *Shrink Wrap* — "plástico" o "empaquetado de plástico") .

Por otro lado, no hay que olvidar que si se trata de un contrato concluido por consumidores el juego del principio de la autonomía de la voluntad en estos contratos no resulta suficiente para garantizar todos los intereses en presencia. De ahí que se busque un foro de protección especial en atención a la parte más débil. Foro que, en el CB, es el de la residencia habitual del consumidor. En cuanto a la ley aplicable el art. 5 CR establece un régimen especial en contratos concluidos por consumidores. La norma está pensada para los consumidores "pasivos", que permanecen en su país de residencia y en él formalizan un contrato internacional de consumo. La determinación de la ley aplicable se fija restringiendo el juego de la autonomía de la voluntad al fin de dejar a salvo la aplicación de las normas imperativas de protección del consumidor previstas por la ley de su residencia habitual. A falta de cláusula de elección, el contrato se rige por la ley de la residencia habitual del consumidor[7].

Es por ello que la Conferencia de La Haya de Derecho Internacional Privado, organización intergubernamental que tiene por objeto la unificación del Derecho internacional privado (esencialmente los conflictos de leyes y los procedimientos y la cooperación judicial internacional) ha llevado a cabo en Ginebra un serie de sesiones sobre cuestiones de competencia judicial y de ley aplicable en relación con el comercio electrónico y las operaciones efectuadas por los intermediarios de *Internet*. En materia de ley aplicable a los contratos "on line", la discusión se centra en la dicotomía entre la ley del vendedor (regla del país de origen de la mercancía) o la ley del comprador (regla del país de recepción). La solución propuesta, y en trámite de discusión, pretende **evitar** esta dicotomía partiendo de un sistema nuevo que se basa en la llamada *Certificación de Sitios* inspirada en los trabajos que la CCI y otras organizaciones privadas están llevando al efecto. Este sistema de *Certificación de Sitios* partiría reglas específicas de protección de los consumidores, incluidas las garantías, así como un sistema de reglamentación de controversias justo, de fácil acceso y gratuito para el consumidor. Si un *Sitio* ha obtenido por ejemplo la Certificación podrá entonces preverse que se aplicará el derecho del país de origen y se dará competencia a los tribunales de ese país, en los casos residuales que no puedan regirse por el sistema autónomo de resolución de diferendos, comprendido en el sistema de *Certificación de Sitios*[8].

---

[6] Este término puede verse ya acuñado en la versión en español de la Propuesta de Directiva relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior (COM 1999 427; 98/0325). Art. 11.1. "Los Estados miembros dispondrán en su legislación que, salvo acuerdo en contrario de las partes y siempre que se trate de profesionales, cuando se pida al destinatario de un servicio que manifieste su consentimiento utilizando medios tecnológico -como por ejemplo, cliquear sobre un icono para aceptar la oferta de un prestador de servicios-, el contrato quedará celebrado cuando el destinatario del servicio haya recibido por vía electrónica una notificación del prestador de servicios acusando recibo de la aceptación del destinatario del servicio". En la Ley Modelo UNCITRAL sobre Comercio Electrónico de 1996 el término no aparece, sino que se habla genéricamente de "comunicación por medios electrónicos" y de "sistemas de comunicación", entendido como todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna u otra forma mensajes de datos [Art. 2 f)]. El subrayado es nuestro. Vid. Vargas Gómez-Urrutia, M., "Comercio Internacional Electrónico y Conflicto de Leyes y de Jurisdicciones en el Cyberespacio", Revista Derecho de los Negocios, Madrid, abril 2000.

[7] Si volvemos a nuestro ejemplo anterior (licencia de uso de Software), es frecuente que Internet sea no sólo la herramienta para formalizar el contrato, sino también el medio para la entrega de la mercancía. La ley elegida, contenida en los formularios de licencia de uso (ya vengan en soporte de plástico del programa o en las condiciones generales del programa que se baja de la red), sólo cedería en el caso de que prive al consumidor de la protección garantizada por las leyes imperativas del Estado de su residencia habitual (art.5.2 CR). Y, en el caso de ausencia de elección de ley, habrá que distinguir si se trata de un contrato internacional "de consumo", en cuyo caso será aplicable la ley de la residencia habitual del consumidor del Software (art. 5.3 CR). Y, si no se trata de un contrato de consumo, en ausencia de elección, se aplicará la ley de la sede de la empresa de Software.

[8] Consultar en <http://cuiwww.unige.ch/~billard/ipilec>. También en el seno de la Conferencia de La Haya el Anteproyecto de Convenio sobre competencia, reconocimiento y ejecución de resoluciones en materia civil y mercantil, contempla la posibilidad de introducir en el art. 7 párrafo 3 que las partes en un contrato concluido por los consumidores pueden convenir la elección del foro mediante una cláusula al efecto, "si esta cláusula ha sido aceptada por un consumidor que reside habitualmente en un Estado que ha declarado que tales acuerdos son válidos respecto de tales consumidores".

Por lo que hace a la situación española de *lege ferenda*, ya existe un anteproyecto de ley de comercio electrónico preparado por el Ministerio de Fomento[9] que pretende, en virtud de los principios comunitarios de reconocimiento mutuo y de control de origen, someter a las prestadoras de servicios por *Internet* en España al requisito (no contemplado en la Posición Común de la Directiva sobre Comercio Electrónico[10]) de inscripción en un registro especial creado al efecto. El anteproyecto español sigue las líneas comunitarias al establecer que los prestadores de servicios serán responsables de los daños y perjuicios causados en el ejercicio de su actividad, en tanto que los operadores de redes y los proveedores de acceso quedan exonerados de responsabilidad por los perjuicios producidos a los contratantes a través del comercio electrónico "si su labor o función ha sido la de meros conductores y transmisores de información". En cuanto al momento de conclusión del contrato "on line", el anteproyecto entiende que éste se considerará perfeccionado en el momento en que el consumidor reciba la aceptación por parte del vendedor. Por lo que hace al **lugar** de celebración del contrato éste será el **domicilio** del **usuario** (**consumidor**) y, en cuanto al tribunal competente para la resolución de conflictos, se establece igualmente que tendrá competencia para conocer el tribunal de la **residencia habitual del usuario-consumidor** (*forum domicilii*). También el anteproyecto pretende potenciar un sistema arbitral de resolución de conflictos por vía telemática, y un régimen de vigilancia y de control para proteger a los usuarios, fijando un procedimiento sancionador con multas muy elevadas para aquellos que incumplan las prescripciones legales.

II. LA PROTECCION DE LA VIDA PRIVADA Y EL COMERCIO ELECTRONICO

Otra de las dificultades que pueden surgir de la utilización de *Internet* y que interesan al DIPr. son las relativas a la precisión de la ley aplicable al derecho a la intimidad y la determinación del tribunal competente para conocer de demandas en petición de responsabilidad civil por los atentados contra los derechos al honor, la dignidad o la vida privada de los individuos. Debido a la difusión global de los mensajes y, por tanto, a la posibilidad de que los efectos del comportamiento ilícito se difundan también de modo global, pueden surgir interrogantes a la hora de determinar con precisión *cuándo* se ha producido la vulneración de un derecho de la personalidad y *dónde* se sufre el daño; y, sobre todo, *quién* responde del daño, habida cuenta de la cantidad de actores que intervienen o pueden intervenir en el *cyberespacio*.

Dos son pues las cuestiones a despejar desde la óptica del DIPr: 1) lugar donde se hubiera producido el hecho dañoso, para la determinación del tribunal competente; y, 2) ley aplicable para la protección del derecho vulnerado.

La dificultad de partida es la determinación en estos supuestos de la *lex loci delicti commissi* que, en principio, opera como regla para la fijar la responsabilidad extracontractual. En efecto, con el uso de *Internet* es factible que se de un concurso potencial de leyes de todos los Estados en donde se hayan producido los siguientes hechos: carga del material ilícito, descarga del mismo, conexión al *Sitio*, recepción del material y, su difusión[11]. Además, la difusión puede darse en un Estado donde el hecho dado no tenga la consideración de una violación de un derecho de la personalidad, o bien puede suceder que el lugar en donde esté situado el suministrador del servicio (y proveedor de los contenidos ilícitos), no tenga establecido un marco jurídico de protección para sancionar como ilícito la carga o tratamiento de dicho material; puede también suceder que, según la ley del lugar donde esté situado el suministrador, se permita la utilización libre de estos contenidos (supuesto de *free use* = libre uso); o, finalmente, que el suministrador de los contenidos esté situado en un Estado pero transmita desde otro cuya legislación sea más permisiva (supuestos de *copyright free-shore* = derechos de copia libre)[12].

---

9 Cf. Otrosí, Publicación informativa de ICAM, marzo 2000, p. 85 y <http://www.abog.net/nti.index.html.>.

10 COM (1999) 427 final 98/0325 (COD) y Posición Común de 8.12.1999.

11 Cf. Carrascosa González, J., "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE", en la Ley-Actualidad Civil, núm. 23 del 2 al 8 de junio de 1997, pp. 531-522.

12 Los casos hasta el presente estudiados por el TJCE vienen a demostrar que el demandante suele elegir como foro de ejercicio de su acción el del tribunal que le ofrezca mejores resultados en orden a la efectiva obtención de dos pretensiones básicas: a) la prohibición y cese de la actividad ilícita; y, 2) la efectiva indemnización por los daños y perjuicios ocasionados. Cf. Bariatti, S., "Internet: aspect relatifs aux conflits de lois", Riv.di diritto internazionale privato e processuale, 1997-3, p. 555.

Desde esta perspectiva conviene advertir con carácter previo, como ha sido puesto de relieve por la profesora P.ABARCA JUNCO[13], que la protección del honor, su contenido y sus formas de tutela implican una cuestión previa de calificación. Se trata de una noción jurídica de contenido indeterminado y alcance relativo. De ahí que, su protección varíe de un país a otro, su alcance sea distinto según las épocas históricas, y su determinación dependa de los valores y principios fundamentales de cada sociedad. Sin embargo, no hay duda de que se trata de un derecho fundamental, recogido en el *Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales*, hecho en Roma el 4 de noviembre de 1950 (art. 8). Esto significa que, por su naturaleza de derecho fundamental, lo que se salvaguarda son valores de la persona (derecho subjetivo de la personalidad) *no su promoción*. Y *ello significa, asimismo, que su protección*, o mejor dicho, el modo en que se protege, lo sea a través de la acción judicial, bien para obtener una tutela judicial efectiva del derecho y reparadora del daño causado, bien para adoptar medidas preventivas que protejan este derecho antes de ser lesionado. La clave está en entender, "que el amparo que otorga el ordenamiento jurídico a estos derechos parte de que el mero hecho de atentar contra ellos presupone un daño, y que este daño no precisa de prueba"[14].

De otro lado, el estudio del derecho comparado nos informa que los ordenamientos jurídicos nacionales del área occidental protegen la intimidad de la vida privada de dos modos distintos, a saber: 1) a través de la responsabilidad civil o penal (países del *common law*); 2) a través de la consideración del interés protegido, *vis a vis* derecho fundamental-derecho subjetivo (países del *civil law*). Esto tiene trascendencia en orden a la determinación del tribunal competente ya que, en el primero de los supuestos, el foro de competencia se determinará por el cauce de la responsabilidad extracontractual, sin necesidad de acudir para la protección al concepto de derecho subjetivo; en tanto que, en el segundo de los supuestos, la especificidad del derecho tutelado exigiría un foro inmediato y especial que asegurara una protección jurisdiccional mayor que la que se otorga a través de los cauces clásicos de la responsabilidad civil[15].

En el grupo de trabajo llevado a cabo bajo los auspicios de la Conferencia de La Haya de Derecho Internacional Privado, no se ha llegado a una conclusión definitiva en materia cuasi delictual. Algunos de los participantes consideran que lo normal es que el foro de la residencia habitual de la víctima del daño coincide con la localización de una parte del daño. En el anteproyecto de Convenio sobre competencia y reconocimiento de decisiones en materia civil y mercantil, no se sigue el foro de la residencia habitual para fijar la competencia, sino que sigue manteniendo la conexión con el **lugar donde ha tenido lugar el daño**. Ello obligaría a la víctima a acudir a varios tribunales; pero también puede demandar en el lugar del establecimiento del editor de la página (el proveedor del *Sitio*), y en este caso el tribunal podría conocer de todos los perjuicios causado por la publicación en cualquier país (en términos de la Sentencia del TJCE que resuelve el caso FIONA SHEVILL).

Nuestro sistema de DIPr., aún admitiendo constitucionalmente que los derechos de la personalidad son derechos subjetivos (sin contenido positivo), no establece un foro de competencia especial de carácter "inmediato"[16] que permita saber de antemano cuál es el tribunal competente para la protección de los derechos de la personalidad, sino que califica las infracciones de estos derechos como supuestos de responsabilidad civil "ex delicto", lo que conduce a la "lex delicti comissi" para saber cuál es la ley aplicable.

Entonces, cómo saber, cómo identificar la norma aplicable para determinar la competencia judicial internacional y, lo mismo, para conocer la ley o el derecho a aplicar?

---

[13] Cf. Abarca Junco, P., "Competencia judicial internacional en materia de difamación por artículos de prensa. A propósito de la sentencia del Tribunal de Justicia de 7 de marzo de 1995 (Fiona Shevill y otros c/ Presse Alliance, S.A.)", Gaceta Jurídica de la CEE, B-113 mayo 96, p. 5; id. "El derecho a la intimidad en el Derecho internacional privado español", en BFD-UNED, núm. 2, 1992, pp. 9-12. Eslava Rodríguez, M. "Responsabilidad extracontractual, gestión de negocios ajenos y enriquecimiento sin causa" (en Calvo Caravaca, A.L., y Carrascosa González, J., Derecho internacional privado. Vol. II), pp. 603-610.

[14] Idem, p. 6.

[15] Sobre los problemas de calificación con crítica a las diferentes alternativas, véase también Carrascosa González, J., op.cit., pp. 517-525.

[16] *Por foro de competencia especial de carácter inmediato entendemos aquel que asegura y atribuye competencia a los tribunales ante* una violación del derecho al honor. Para que se actualice este foro es necesaria una vinculación suficiente entre los hechos en que se basa la petición de protección jurisdiccional y el ámbito territorial del tribunal ante el cual se acude.

Competencia judicial. Según nuestro sistema, la competencia judicial internacional se encuentra regulada para estos supuestos en el art. 5-3 del CB (*"El demandado domiciliado dentro de territorio de un Estado contratante puede ser demandado en otro Estado contratante [...] 3. En materia delictual o cuasi delictual ante el juez* ***del lugar donde se haya producido el daño****"*; y en el art. 22.3 LOPJ (*"En el orden civil los tribunales y juzgados españoles serán competentes [...] 3. En materia de obligaciones extracontractuales, cuando el* ***hecho del que deriven haya ocurrido en territorio español o el autor del daño y la víctima tengan su residencia habitual común en España***). Y, por lo que hace a la ley aplicable, la norma de conflicto es la contenida en el art. 10.9-I del Código Civil (*"Las obligaciones no contractuales se regirán* ***por la ley del lugar donde hubiere ocurrido el hecho del que deriven****"*).

Los problemas que se plantean para la **concreción espacial de la conexión** (lugar del hecho que causa el daño o lugar donde éste se ha producido) obedecen a que "ese lugar" es incierto. El propio TJCE así lo ha reconocido (Caso BIER)[17], ya que el lugar del evento causal puede ser considerado en un caso de difamación por medio de una publicación tanto el lugar de edición como el de difusión; y, el lugar del perjuicio pueden ser varios, al ser varios países donde se divulgan los contenidos. Por tanto, el demandante puede emplazar al demandado ya sea en el lugar donde se ha producido el hecho causal como en el lugar del daño. En Sentencia posterior el TJCE, reafirmando la jurisprudencia del caso BIER, considera, además, que lugar del hecho causal es el del establecimiento del editor de la publicación, y lugar del daño son los lugares de difusión de la misma. Cuestión diferente es la concerniente a los límites a la competencia del tribunal que conoce de la causa. En la Sentencia del TJCE de 7 de marzo de 1995 (Caso FIONA SHEVILL), se ha precisado el alcance y límites del art. 5-3 del CB en el sentido de que, **si se demanda ante el tribunal del lugar de la edición, éste podrá conocer de todos los perjuicios ocasionados por la distribución de la publicación en los demás países.**

Y, si se demanda ante el tribunal del lugar de la distribución, sólo podrá conocer de los perjuicios ocasionados en su territorio[18].

Por lo que hace al derecho interno español, la norma contenida en el art. 22-3 de la LOPJ atribuye competencia a los tribunales españoles, según hemos visto anteriormente, cuando el **hecho del que derive la obligación haya ocurrido en España o el autor del daño y la víctima tengan su residencia habitual común en nuestro país, aunque el hecho haya tenido lugar en el extranjero**. Esta norma trata de otorgar mayor protección a los residente en territorio español, ampliando el volumen de competencia atribuido a los tribunales españoles. Este dato, en consonancia con el art. 10.9 del C.civil, relativo a la ley aplicable a las obligaciones extracontractuales, hace que el tribunal español pueda conocer de asuntos en los que el hecho generador no hubiere ocurrido en España y que, a tenor de la norma conflictual, el derecho aplicable sea una ley no española[19].

No es nuestra finalidad hacer una exposición de las diversas teorías cultivadas, sobre todo en la doctrina alemana y francesa[20], en orden a la concreción del "lugar donde se hubiera producido el hecho dañoso" y "lugar donde se sufre el daño". Lo que a nuestra reflexión interesa en este momento (responsabilidad por la violación de un derecho de la personalidad llevada a cabo por *Internet*) es la correcta identificación de los operadores-actores de la Red, ya que esto resulta esencial para la determinación de la competencia judicial y de la ley aplicable al supuesto en la especie[21].

---

[17] Sentencia Bier vs. Mines de potasse d´Alsace, de 27 de febrero de 1976, que marcó la directriz general en la interpretación del art. 5-3 CB al determinar que el lugar debe ser entendido en el sentido de contemplar a la vez el lugar donde el daño ha sobrevenido y el del evento causal . Sobre esta sentencia ver Abarca Junco, P., "Competencia judicial internacional en materia de difamación por artículos de prensa...", op. cit., p. 7.

[18] Cf. Abarca Junco, P., "Ley aplicable a la responsabilidad por daños", en Vv.Aa., Derecho Internacional Privado, (E. Pérez Vera, Dir), Capítulo XXVII, U.D. II., UNED, Madrid, 1998, p. 308; Calvo Caravaca, A.L., y Carrascosa González, J., Derecho internacional privado. Vol. II., pp. Los ilícitos a distancia y la responsabilidad por daños en las intromisiones ilícitas en los derechos de la personalidad. Los autores distinguen entre intromisiones ilícitas cometidas mediante mass media e intromisiones ilícitas en relación con el tratamiento de datos.

[19] Ibidem.

[20] Cf. Carrascosa González, J., "Circulación internacional....,"op.cit., pp. 523-524.

[21] El esfuerzo para identificar a un responsable de unos contenidos ilícitos albergados en un determinado Sitio de Internet no es nada fácil, y menos cuando se trata de un medio nuevo con técnicas muy sofisticadas y cambiantes. Es por ello que resulta útil, sobre todo para quienes somos profanos en esta "cybernebulosa", conocer quiénes son los actores de Internet y qué función cumplen. La reciente sentencia de la Cour d´Appel de Paris de 10 de febrero de 1999 es un buen ejemplo de lo que ahora exponemos. Cf. Rec. Dalloz, 1999, 26ª Ch. Jurisprudence, pp. 389 y ss. (con comentario de N. Mallet-Poujol).

La reciente decisión de la Cour d´Appel de Paris resulta de interés para el DIPr. por cuanto: a) nos proporciona algunas pautas para reflexionar sobre la concreción de un punto de conexión en el *cyberespacio*; y, b) localizado ese punto de conexión podremos saber a qué tribunal atribuir la competencia judicial internacional y qué ley aplicar a casos similares en los que no se conozca la ubicación del *Sitio-Internet* ni la persona que suministre el servicio o los contenidos. Sumarizando el problema planteado:

en el caso de autos, la perjudicada por la información distribuida por *Internet* (la modelo francesa), desconocía al verdadero suministrador del servicio y de los contenidos; sabía el *Sitio* de la *WEB* en donde se alojan éstos, pero este *Sitio* era una mera dirección electrónica (**<www.altern.org>**;

- ✓ pide prueba de expertos en informática y consigue determinar quién administra tal Sitio;
- ✓ esta persona es el Sr. Valentin X; con un domicilio conocido ;
- ✓ ha dado un primer paso: saber quién administra el Sitio, cuál es su domicilio y fijar un punto de conexión espacial que le permita determinar el lugar de la edición/lugar de la distribución.

Pero, otros pasos son necesarios a continuación, ¿cómo determinar la responsabilidad de los diversos actores de la Red? Para poder demandar es preciso saber a *quién* o a *quiénes* demandar (legitimación pasiva), *dónde* demandar (para conocer el *forum*) y *qué* demandar (para aplicar el *ius*). Para ello, en nuestro caso, se plantearon varias cuestiones previas por parte del demandado relacionadas todas ellas con la exoneración de su responsabilidad. Ello nos lleva a preguntarnos sobre un dato nuevo. Es necesario conocer "a priori" las funciones que cumplen en la Red los diferentes agentes u operadores esto es: los suministradores (proveedores) —el que provee el acceso a la Red, el que provee el *Sitio-Internet* y lo mantiene, alojando contenidos diversos y, el que provee los contenidos, que puede o no coincidir con el que alberga—, todo con el fin de identificar sus deberes y los mecanismos de determinación de sus responsabilidades.

Dicho de otro modo, ¿quién es quién en la Red? Tomando las definiciones de un informe del Consejo de Estado francés de 1998, y a grandes rasgos, un **suministrador de *Acceso*** es el que ofrece al público un servicio de conexión a Internet por medio de sus propios ordenadores, los cuales, a su vez, están conectados a Internet. Un **suministrador de un *Sitio***, es aquel que asegura un servicio de almacenamiento y tratamiento de contenidos en la memoria de un ordenador conectado a Internet. Y, un **suministrador de *Contenidos,*** es aquel que introduce un contenido en el Sitio, esto es una base de datos, o un grupo de discusión, o unas imágenes, con el fin de que sea de acceso al público. Estos últimos se suelen especializar por materias, distinguiéndose dos grandes grupos: las comerciales (prensa, editoriales, bancos, comerciantes, etc.); y, las no comerciales (universidades, particulares, gobiernos, etc.). En la práctica, las funciones de los suministradores de un *Sitio* y de los suministradores de contenidos se acumulan con frecuencia en un mismo proveedor, de ahí que, en estos casos, su distinción, a efectos de responsabilidad, no tendría más fin que el puramente funcional.

El razonamiento de la Cour d´Appel de Paris en la sentencia que traemos como ejemplo parece estar inspirado en la llamada tesis de la "responsabilidad en cascada", que hace recaer en el difusor de los contenidos ilícitos la responsabilidad de la elaboración de un mensaje, pese a no ser él mismo el autor del mensaje. Esta responsabilidad se liga o une al acto de publicación y es una consecuencia del principio o deber de verificación y de vigilancia del director de toda *publicación,* no importa cuál sea el soporte técnico que la contenga[22]. Al vincular la "culpa" del suministrador de un *Sitio* de Internet que alberga contenidos ilícitos con un **deber de vigilancia o de verificación de los contenidos** la Corte de Apelación francesa está aparentemente calificando tal conducta como una obligación de garantía, lo que justificaría la responsabilidad civil objetiva frente a terceros del suministrador del *Sitio* que alberga los contenidos por los daños causados a los mismos. En esta materia, -atentado contra la intimidad personal-, el mecanismo de protección se actúa en el momento en que se constata la violación del dere-

[22] *En el caso del suministrador de un sitio de Internet, el Consejo de Estado francés ha entendido que este profesional tiene un deber de* vigilancia de los contenidos que le son propuestos para introducir en línea, y que corresponderá a la jurisprudencia determinar en cada caso "los standars de comportamiento razonables exigibles a dicho profesional".

cho subjetivo, según ha sido expuesto anteriormente, sin que sea necesario probar la falta. Autor y editor (en este caso, suministrador de los contenidos y suministrador del *Sitio* que alberga tales contenidos) son condenados conjuntamente ya que el acto de la publicación (edición y albergue en términos de *Internet*) es lo que fundamenta la obligación de reparación del daño. Y, en consecuencia, es esta **conexión espacial la que permitirá, concretar el tribunal que debe conocer de la demanda (lugar de edición y lugar de difusión).**

Ley aplicable. Queda por dilucidar la ley aplicable (**lugar donde se ha producido el daño).** La centralización de competencia judicial propuesta por el Grupo de Trabajo de la Conferencia de La Haya de Derecho Internacional Privado, no excluye que el juez tenga que concretar el **lugar donde se produce el daño para conocer el derecho aplicable**. Como hemos señalado anteriormente, para unos ese lugar es el de la difusión de la publicación, lugar que también es considerado como el lugar donde se genera el daño. Otro sector doctrinal considera que el lugar del daño equivale al lugar del domicilio de la víctima; ya que es en su lugar de residencia en donde hay que localizar un perjuicio que está tan ligado a su persona (el ataque a su vida personal y a su intimidad).

La posible admisión por parte del grupo de trabajo de la Conferencia de La Haya de DIPr., del **lugar de residencia habitual de la víctima en aras a la determinación del derecho aplicable** presentaría la ventaja de la aplicación de una única ley a todos los problemas relativos a la protección del derecho a la vida privada, como ha sido puesto de relieve por un amplio sector doctrinal. Por el momento, y dados los términos de nuestro artículo 10.9 C. civil, aplicable a todas las obligaciones no contractuales que no tengan una norma específica de DIPr. (interno o convencional), la ley aplicable a la responsabilidad extracontractual en nuestro país es la "loci delicti comissi" que se refiere al "lugar donde hubiere ocurrido el hecho de que deriven". Ello quiere decir que el tribunal español, en principio, tendrá que localizar materialmente los hechos para saber el derecho a aplicar.

Empero, la aplicación rígida de esta norma a todos los supuestos y cuestiones puede "eludirse" atendiendo a la naturaleza de la cuestión planteada y mediante el ejercicio previo de la calificación, según ha puesto de relieve la doctrina. Es decir, a la "lex loci delicti comissi" se le pueden "poner" excepciones dependiendo del tipo de ilícito de que se trate. Y, en el ámbito que estamos tratando ahora, no cabe duda que si incluimos el derecho al honor como un derecho de la personalidad *vis a vis* derecho fundamental eludiríamos la *lex loci* para aplicar la *lex fori* como norma procesal (porque la protección de los derechos subjetivos son indisociables de la adopción de medidas judiciales que lo sancionan) y como norma imperativa (porque el derecho al honor, como derecho fundamental, tiene una importancia de carácter esencial para el ordenamiento del foro).

Ahora bien, si consideramos que el derecho al honor es un derecho que forma parte del estatuto personal, entonces tendríamos que acudir a la ley personal de la víctima como aplicable al supuesto en especie (ley de la nacionalidad). No es nuestro interés en estos momentos debatir sobre los interesantes argumentos doctrinales que en defensa de una u otra postura se han concitado. Quede simplemente puesto de relieve que las nuevas tendencias interpretativas de las normas de DIPr. buscan eminentemente el objetivo material de la Justicia, y para ello ofrecen técnicas de reglamentación "distintas" a las clásicas.

Si el objetivo material en los casos en los que se viola el derecho a la intimidad a través de una técnica tan sofisticada como *Internet* lo vinculamos con el principio del *"favor laesi"*, modulado por el otro principio, también fundamental, del derecho a la información, entonces, en nuestra opinión, el tenor de la norma contenida en el art. 10.9 C.civil resulta de difícil concreción para el supuesto en la especie. No es que sea imposible la localización para concretar el lugar del daño, pero es precisamente la multiplicación exponencial de ese lugar del daño la que nos hace pensar que el problema que apuntamos necesita de una regulación especial. ¿Cómo? Quizá flexibilizando la norma de conflicto al objeto de que la víctima pueda: a) en materia de competencia judicial, elegir el foro; y, b) en materia de ley aplicable, teniendo en cuenta de que se trata de daños plurilocalizados, en lugar de seguir una localización material ("lugar donde hubiere ocurrido el hecho de que deriven"), sugerir que el lugar donde éstos se lesionen se vincule con la residencia de la víctima[23].

23 Esta es la propuesta de P. Bourel que entiende que esta conexión es fija, cierta y previsible; atiende a criterios jurídicos y sociológicos; y, concilia adecuadamente la significación individual y social de los derechos protegidos (derechos de la personalidad). Cf. Bourel, P., "Du rattachement de quelques délits spéciaux en droit international privé", RCADI, 1989, vol. II, T. 214, pp. 251-398. Y del mismo autor, "Notas a la Sentencia de Minas de Potasio de Alsacia, en RCE, 1977, pp. 568 y ss.

III. LA INTIMIDAD INFORMATICA (PRIVACY) Y EL COMERCIO ELECTRONICO (LA PROTECCION DE DATOS PERSONALES)

Lo que constituye el objeto de reflexión en este inciso no es la protección de los derechos de autor sobre las bases de datos (tema que tiene que ver con el derecho internacional de la propiedad intelectual en un mundo digital (*International Copyright In A Digitally Networked World*), y que merece un estudio más pormenorizado. El aspecto que analizaremos se circunscribe a las protección de los datos de carácter personal; es decir, el tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar. Dicho de otro modo, "el derecho a la autodeterminación informativa".

El llamado derecho a la *autodeterminación informativa* (*informationelle Selbstbestimmungsrecht*[24]) implica, como ha señalado LUCAS MURILLO[25], "el poder jurídico de rechazar intromisiones ilegítimas en la esfera protegida, y correlativamente, determinar libremente y dentro de ella, la propia conducta". La técnica de protección de este derecho combina el propio poder del individuo frente a terceros (limitaciones y prohibiciones) y el contenido de los datos que se protegen, que no tienen por qué ser íntimos, sino que basta con que sean personales[26]. De ahí que, como afirma el anterior autor, el ámbito de protección de este derecho es más amplio que el propio derecho a la intimidad. Lo que nos interesa destacar ahora, si quiera de modo sumario, es que la protección de los datos personales contenidos en las llamadas bases de datos, tiene un marco regulador específico en el derecho español y, de igual modo, la transmisión internacional de datos personales goza de una "cierta autonomía" consecuencia de la regulación convencional de que ha sido objeto.

Aunque el cuerpo internacional de reglamentación del "movimiento internacional de datos" no es muy extenso, los cuatros textos más relevantes que abordan la ordenación de la protección de datos personales son:

1. La *Recommendation du Conseil concernant les Lignes Directrices régissant la protection de la vie privée et les flux transfrontières des donnèes de caractère personal*, de 23 de
2. septiembre de 1980/ Guideline on the Protection of Privacy and Transborder Flows of Personal Data (23rd. September, 1980)[27]
3. El Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España por Instrumento de 27 de enero de 1984 (BOE, de 15 de noviembre de 1985).
4. Los Principios rectores para la reglamentación de los ficheros computerizados de datos de carácter personal. E/CN.4/1990/72, de 20 de febrero de 1990.
5. La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Los textos internacionales antecitados poseen ámbitos de aplicación diferentes y por ende, grados de obligatoriedad distintos. En cualquier caso, sí es posible encontrar elementos comunes a todos estos textos. El más importante a nuestro propósito de estudio, es que la cuestión del movimiento internacional de datos pasa por considerar que **"entre dos países afectados por un flujo de datos a través de sus fronteras, la información debe circular libremente, como en el interior de cada uno de los territorios respectivos, siempre y cuando el nivel de protección otorgado al individuo en cada uno de los ordenamientos afectados sea**

---

[24] Configurado por la famosa Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983, como la facultad del individuo de decidir básicamente por sí mismo cuando y dentro de que límites procede revelar situaciones referentes a su vida privada. Cf. Boletín de Jurisprudencia Constitucional, núm. 33, 1984, pp. 126 y ss.

[25] Lucas Murillo, P., *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990, pp. 117-118.

[26] Ruiz Miguel, C., "El derecho a la intimidad informática en el ordenamiento español", RGD, vol. 607, abril 1995, p.3211.

[27] Se puede consultar "on line" en <http//: www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm>.

similar"[28]. Ello obliga a proponer una legislación uniforme internacional o al menos homogénea que parte del principio de **"nivel de protección equiparable"**, como cláusula general aplicable. La consideración de tal principio como cláusula general no es cuestión baladí, ya que su concreción se hace depender de un criterio valorativo, *concretu casu*, criterio que se modula a través de una doble vía: por un lado, objetivando el principio; y, por otro, permitiendo la diversificación de las autoridades intervinientes en la adopción de las decisiones. Sobre estos dos aspectos nos detendremos posteriormente.

Constitucionalmente, en España, la dignidad de la persona es un derecho fundamental, por lo que ese llamado *derecho a la autodeterminación informativa* en nuestro ordenamiento jurídico, sería un derecho vinculado al derecho a la intimidad, protegido por el art. 18.4 de la Constitución[29]. Debe hacerse notar que la nueva Ley Orgánica de Protección de Datos no hace referencia a este artículo, a diferencia de la antigua LORTAD[30].

Por lo que hace a la normativa jurídica de rango no constitucional, el marco de ordenación del tratamiento informático de datos de carácter personal "en casos internacionales" se encuentra en los siguientes cuerpos normativos: a) *Convenio 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* (BOE 274, de 15 noviembre 1985[31]); b) *LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal* (BOE del 14) que viene a derogar a la Ley Orgánica para la Regulación del Tratamiento automatizado de Datos de Carácter Personal (LORTAD) 5/ 1992, de 29 de octubre (BOE 262 de 31 octubre 1992), desarrollado por RD 1332/1994 de 20 de junio y RD 428/1993 y RD 994/ 1999, de 11 de junio, (que continúan en vigor en tanto no se aprueben por el Gobierno las disposiciones reglamentarias para la aplicación y desarrollo de la nueva Ley (Disposición Final Primera de la LO 15/1999); c) *Directiva 95/46/CE de 24 de octubre de 1995*, que viene a complementar el Convenio 108, con un alcance es más restringido al limitar su ámbito de aplicación material y geográficamente "al tratamiento de datos personales que se desenvuelven dentro del ámbito de aplicación del derecho comunitario" (Considerando 12)[32]; y, d) *Convenio de Aplicación de los acuerdos de Schengen, que crea el Sistema de Información Schengen (SIS)* (Protocolo de adhesión de España al Acuerdo de Schengen de 14 de junio de 1985 (España firma el Protocolo en Bonn el 25 de junio de 1991 (BOE, 30 de julio de 1991).

La objetivación del **principio "nivel de protección equiparable"**, ha quedado recogida en la Directiva 95/46/CE (objeto de transposición en la LO 15/1999) al precisar los elementos que han de tomarse en cuenta para evaluar la idoneidad de la protección ofrecida por un país tercero: naturaleza de los datos, fin o fines del

---

28 Ripoll Carulla, S., "El movimiento internacional de datos en la Ley española de protección de datos", op.cit. p. 315.

29 Vid. Herrero-Tejedor, F., Honor, Intimidad y Propia Imagen, Colex, Madrid, 1994, pp.21-34; pp. 51-72. Y en relación con las libertades del art. 20.1 de la Constitución, pp. 111-136.

30 La antigua LORTAD tenía por objeto el desarrollo del artículo 18.4 de la Constitución (limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos). En el caso de la nueva LOPD, su objeto no es el desarrollo del citado artículo sino la de garantizar y proteger, por lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar (art. 1º).

31 El Tribunal Europeo de Derechos Humanos ha abordado el problema de las protección de los datos personales en diversas sentencias. Concretamente ha analizado los datos policiales, los datos médicos, los datos judiciales y los datos obrantes en archivos administrativos, tanto en relación con los mecanismos de obtención como por las cesiones y divulgación que de ellos puede realizarse. Así: Datos policiales: Asunto Klaus y otros contra Alemania (STEDH de 6 septiembre 1978); Asunto Malone contra Reino Unido (STEDH de 2 de agosto de 1984; Asunto Huvig contra Francia y Asunto Kruslin contra Francia (STEDH, de 24 abril 1990); Asunto Lüdy contra Suiza (STEDH de 15 de junio de 1992); Asunto Van Mechelen y otros contra los Países Bajos (STEDH de 23 abril 1997); Asunto Laender contra Suecia (STEDH de 26 de marzo de 1987); Datos médicos: Asunto M.S. contra Suecia (STEDH de 27 de agosto de 1997); Asunto Anne-Maire Andersson contra Suecia (STEDH de 27 de agosto de 1997); Datos judiciales: Asunto Foucher contra Francia (STEDH de 18 de marzo de 1997); Datos obrantes en archivos administrativos: Asunto Gaskin contra Francia (STEDH de 7 de julio de 1989). Cf. Freixes Sanjuán, T., "La protección de los datos automatizados por el Tribunal Europeo de Derechos Humanos", en Encuentros sobre Informática y Derecho 1997-1998, (Coord. Davara Rodríguez, M.A.), Facultad del Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1998, pp.33-49.

32 Sobre esta Directiva, vid, Cámara Lapuente, S., "El nuevo derecho sui generis sobre las bases de datos", en Actualidad Civil, núm. 3, semana del 18 al 24 de enero de 1999, pp. 49-107; Carrascosa González, J., "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE", Actualidad Civil, núm 23/ 2-8 junio 1997, pp. 509-539; Donnecker, E y Bascón, C., "Sanciones contra la violación de los derechos de autor en las bases de datos", en Poder Judicial, núm. 53, 1999, pp. 107-126; Prieto Gutiérrez, J.M., "La Directiva 95/46/CE como criterio unificador", en Poder Judicial, núm. 48, 1997, pp. 165-233.

tratamiento, normativa vigente en el país en cuestión, normas profesionales en vigor, códigos de conducta y prácticas que el tercer país posea; proporcionalidad de los datos, transparencia en la recogida de la información, seguridad y responsabilidad de los encargados de los ficheros, derechos de acceso, rectificación y oposición, tipos específicos de tratamientos (datos sensibles, publicidad directa) y, desde luego, será especialmente útil considerar si el país en cuestión es o no Parte del Convenio del Consejo de Europa sobre la materia.

En cuanto a las **autoridades intervinientes** para evaluar la idoneidad de la protección y decidir en su caso la prohibición de la transmisión, de acuerdo con la Directiva corresponde a cada Estado miembro fijarla[33] (*transposición en los arts 35-42 LO 15/1999*) y a la Comisión comprobar a su vez tal extremo. La normativa internacional prevé la posibilidad de establecer **excepciones** al principio de nivel de protección equiparable, de modo que, en determinadas ocasiones, sea posible transmitir datos personales a terceros países aun cuando éstos no cuenten con un adecuado grado de protección. *Grosso modo*: cuando el interesado haya dado su consentimiento, bien de modo expreso, bien a través de una cláusula contractual (recogido en el art. 34 e) de la LO 15/99); y, cuando resulte necesaria para la salvaguarda de un interés público importante o del interés vital del interesado (art. 34 b) en relación con los incisos c), f), h) del mismo).

La LO 15/1999, de 13 de diciembre, al trasponer la Directiva, concreta su ámbito de aplicación material a *los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado* (art. 2). Y por lo que hace a su **ámbito de aplicación espacial** el art. 2 circunscribe la aplicación de la ley a tres supuestos: a) cuando los datos hayan sido tratados en territorio español y en el marco de actividades de un establecimiento del responsable del tratamiento; b) cuando el responsable del tratamiento no esté establecido en territorio español pero le sea de aplicación la legislación española por el juego de las normas de Derecho internacional público[34]; y c) cuando el responsable del tratamiento no esté establecido en territorio de la UE y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen sólo con fines de tránsito.

Desde la óptica internacionalprivatista se plantean algunas dudas. Dudas que, como cabría de esperar, basculan en torno a dos órdenes de cuestiones: a) la competencia del tribunal español para conocer de las demandas sobre responsabilidad por la violación de la *privacy* en la recogida, tratamiento y transmisión de sus datos personales; y, b) la ley aplicable a la recogida, tratamiento y trasferencia de datos personales.

Competencia judicial internacional de los tribunales españoles

Por aplicación del Convenio de Bruselas de 1968, son dos los foros de atribución de competencia que permitirían conocer de demandas en materia delictual y cuasi delictual a nuestros tribunales: a) el foro especial del art. 5,3, si España fuera el lugar donde se hubiera producido el hecho dañoso; y, b) el foro general del art. 2, si el demandado tiene su domicilio en España. De no ser de aplicación del Convenio de Bruselas, la competencia para conocer vendrá atribuida por el art. 22,3 de la LOPJ, cuando el hecho del que deriva la responsabilidad haya ocurrido en España y, por el mismo precepto, cuando el autor del daño y la víctima tuvieran su residencia común en España.

En este ámbito concreto del tratamiento de datos personales resulta de aplicación lo que en las anteriores reflexiones hemos tratado en torno a la precisión del "lugar de producción del hecho dañoso" (según CB), y "hecho del que deriva la responsabilidad" (según LOPJ). ¿Qué deberemos entender por "lugar de producción hecho dañoso" y por "hecho del que deriva la responsabilidad" en relación con los datos tratados por medios

---

33 En España, la Agencia de Protección de Datos. Sobre sus funciones, proyectos, análisis de valoraciones de problemas específicos, legislación y otras actividades de la APD, ver Agencia de Protección de Datos, Memoria 1998, Madrid, 1999.

34 En este inciso el legislador español ha transcrito la literalidad del artículo 4.2 de la Directiva que señala la aplicación del derecho nacional de un Estado miembro "cuando el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público". Sin embargo queda confusa la referencia al Derecho internacional público. *En nuestra opinión, si el responsable de un fichero no está establecido en un país comunitario, y sin embargo* se le aplica el derecho de ese país comunitario, la remisión sólo podría hacerse en virtud de una norma conflictual, sea de origen interno sea de origen convencional.

electrónicos, a los efectos de concreción del foro? Para despejar esta cuestión, y siguiendo la misma línea argumentativa seguida en nuestro anterior epígrafe, podemos preguntarnos a *quién* demandar, *dónde* demandar y *qué* demandar.

En el caso del tratamiento de datos de carácter personal la responsabilidad del que trata los datos es más fácilmente delimitable que en el caso de *Internet*, ya que las disposiciones legales aplicables establecen una regulación muy pormenorizada de los ficheros en donde se almacenan los datos y sus clases.

Si el fichero está situado en España o en alguno de los Estados miembros de la Unión Europea el **responsable** y el **encargado** del tratamiento son fácilmente identificables. Como el criterio de la ubicación del fichero es el que se sigue para la determinación del responsable, entonces la concreción del "lugar de producción del hecho dañoso" coincidirá con el lugar de ubicación el fichero. Veamos *quién es quien* para ser demandado y *dónde* demandar:

¿Quién? **Responsable del tratamiento** o del *fichero* es "la persona física o jurídica de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento" (art. 3 d) de la LOPD). En tanto que el **encargado del tratamiento** es "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" (art. 3 g) LOPD). El derecho a la indemnización como consecuencia del incumplimiento de lo dispuesto en la LOPD se otorga a "los interesados" **contra el responsable o el encargado del tratamiento (art. 19,1 LOPD).** Y, ¿dónde está el fichero? La propia LOPD establece en su Título IV los requisitos para la creación de ficheros, tanto de utilidad pública como privada, exigiéndose en el primer caso una inscripción registral bajo el control de la Agencia de Protección de Datos en donde se hace constar "la dirección de la ubicación del fichero". Y, en el segundo supuesto (fichero de utilidad pública), su creación, modificación o supresión se hace por medio de disposición general publicada en el BOE, con indicación de las personas responsables y lugar de ubicación. **Todo ello reconduce al lugar de ubicación del fichero como lugar en donde se produce el hecho dañoso (en términos del CB) y "lugar del hecho del que deriva la responsabilidad" (en términos LOPJ).**

¿Dónde demandar? Parece claro que si el fichero está establecido en territorio español y la violación del derecho personal se produce en España por datos tratados en España, nuestros tribunales podrán conocer en los términos anteriormente señalados.

Ahora bien, ¿qué sucedería si el responsable del tratamiento no está establecido en territorio de la Unión Europea, pero utilice en el tratamiento de datos medios situados en territorio español? La respuesta la da la propia LOPD al establecer la obligación de designar un representante en España (art. 5 inciso 1 *in fine* LOPD). Ello significa que también en este caso le será de aplicación lo dispuesto en la legislación española, por imperativo del art.2 c) del mismo cuerpo legal (ámbito de aplicación). Y por ende, tendrán competencia nuestros tribunales para conocer.

Finalmente, si el fichero no está establecido en España ni en territorio de la Unión Europea, ni tampoco se han utilizados medios situados en territorio español, ¿podría conocer el tribunal español? Hipotéticamente podemos pensar en dos situaciones posibles: a) sumisión de las partes con renuncia expresa a todo fuero o jurisdicción que pudiera corresponderles (*prorrogatio fori*); y b) que tanto autor del daño como víctima tengan su residencia en España (art. 22,3 LOPJ). En el primer caso, entendemos que el tribunal español podría conocer en base al siguiente razonamiento: bien para evitar la denegación de justicia o bien porque, declarándose competente, pudiera ser aplicable la ley española al fondo del asunto y ésta fuere más favorable al interés de la víctima o del perjudicado (criterio del *favor laesi*). En el segundo supuesto, nos parece clara la competencia, aunque la hipótesis es difícil de que se de. Cuestión diferente sería la reconocimiento y ejecución de ese sentencia en otro país, punto que no trataremos en esta exposición.

Ley Aplicable.Establecida la homogeneidad en el tratamiento y transmisión de los datos personales, la Di-

rectiva 95/46/CE[35], ha optado por fijar como criterio de conexión para la determinación del derecho aplicable al tratamiento de **datos la ley del país donde se halle situado el establecimiento del responsable de dicho fichero**. En lo sucesivo identificaremos este criterio como el de la **"ubicación del fichero"**, siguiendo la terminología de J. CARRASCOSA.

Debe recordarse que esta norma de conflicto rige sólo para los países miembros de la UE; y, como tales países tienen un nivel similar de protección de la *privacy* de los individuos frente a la informática, la aplicación de un derecho extranjero de uno de los Estados miembros no debe en principio ofrecer problemas sobre la adecuada protección del perjudicado. Debe hacerse notar que este *nuevo* punto de conexión -"ley del lugar de la ubicación del fichero"-, es distinto a la regla *lex loci delicti commisi*[36]. No sigue la idea de lugar donde se ha generado el daño sino que identifica los procesos productivos del tratamiento de datos reconduciéndolos a un solo lugar: **donde esté establecido el fichero**. En consecuencia, da igual que el fichero esté en Francia y que los datos se traten en España; siempre se aplicará la ley de la *ubicación del fichero*

Pero también demuestra algunas carencias. Por ejemplo, si los ficheros están situados fuera de la UE el criterio no entra en juego ya que en principio éste sólo es aplicable a los supuestos *ad intra*[37]. Pese a ello, las leyes internas de los Estados y la propia Directiva ofrecen parámetros de solución siguiendo el criterio del "nivel de *protección adecuada" como barrera para garantizar la privacy de los individuos frente al uso de la informática.*

En este punto nos interesa destacar los artículos que la nueva Ley Orgánica de protección de datos personales[38] dedica al movimiento internacional de datos. El Título V de la nueva Ley, titulado "Movimiento internacional de datos" destina dos artículos (artículos 33 y 34) a la ordenación de dicho movimiento internacional. Pese a la brevedad del Título, el hecho de que la Ley Orgánica, al igual que la anterior LORTAD, haya dado autonomía a la cuestión es un reflejo de la importancia de la misma[39]. Ambos preceptos están inspirados en el art. 12 del Convenio de Estrasburgo de 1981 (Convenio 108), y en la Directiva 95/46/CE, de 1995, de ahí que,

---

35 Su objetivo es lograr en el espacio de la UE una "libre circulación de datos personales" susceptibles de tratamiento informatizado o que han sido tratados informáticamente, y para ello armonizar el nivel de protección que ofrecen las distintas legislaciones de los Estados miembros. La Directiva distingue dos tipos de relaciones jurídicas: 1) las administrativas, entre los responsables y los encargados del fichero de datos personales y la Autoridad Pública; y, 2) las particulares, derivadas del tratamiento automatizado de datos. En el primer supuesto, la omisión de los controles administrativos que las autoridades públicas establecen, dará lugar a sanciones administrativas contra los responsables de los ficheros. En el segundo supuesto, los perjuicios que se causen a los particulares por parte de los responsables de los ficheros, dará lugar que la pertinente "reparación del perjuicio causado". En ambos supuestos el criterio para la determinación de la ley aplicable es *único: la de la ubicación del fichero. Vid. Carrascosa González, J., "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE"*, op.cit. p. 533.

36 Que es la que recoge el artículo 10.9.I C.c., con carácter general y que la LO 15/1999, en sus artículos 33 y 34, "modifica" su aplicación en ciertos supuestos; en concreto: cuando la lex loci delicti commisi señalada por la norma conflictual española comporte la aplicación *de un ordenamiento extranjero que no proteja la privacy del individuo o de los sujetos afectados con un nivel equiparable al que proporciona* la LO 15/1999.

37 La Directiva en estos casos establece varios parámetros. En primer lugar no juega el criterio de la "ubicación del fichero" para la determinación de la ley aplicable al tratamiento de datos porque éste sólo es válido para los países de la UE. Por ello entrarán en juego las *reglas de DIPr. autónomas, propias de cada Estado miembro. En el caso español, el art. 10.9.I C.c (ley del país donde se lleva a cabo el tratamiento de datos)*, siempre que la misma ofrezca un "nivel equiparable" de protección (art. 33 LO 15/1999). La Directiva se refiere a nivel de "protección adecuada" ofreciendo varios parámetros (arts. 25.2 y 25) para su concreción. En el caso de que la ley extranjera designada por la norma de conflicto autónomo sea de un país que no garantiza ese nivel de la privacy frente a la utilización de la informática, la *transferencia está prohibida y si se produjera generaría las responsabilidades por parte de cedente y cesionario. La ley aplicable a dicha* responsabilidad será la del país donde radica el establecimiento del responsable de la cesión internacional de datos.

38 Davara Rodríguez, M.A., "Los principios de protección de datos y los derechos de las personas en la nueva Ley Orgánica de Protección de Datos de Carácter Personal", en Actualidad Informática, Aranzadi, núm. 34, enero 2000, pp. 1-8; Fernádez López, J.M., "La nueva Ley de protección de Datos de Carácter Personal de 13 de diciembre de 1999. Su por qué y sus principales novedades", en Actualidad Informática Aranzadi, núm. 34, enero 2000, pp. 1y 8 a 9; Del Peso Navarro, E., "Principales diferencias entre la nueva Ley de Protección de Datos y la LORTAD", idem, pp. 11-15.

39 Cf. Carrascosa González, J., "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE", op.cit., pp. 527-531; Ripoll Carulla, S., "El movimiento internacional de datos en la Ley española de protección de datos", Informática y Derecho, 6-7, CRE-UNED, 1995, pp. 313 y ss. Ambos referentes a la antigua LORTAD, pero útiles habida cuenta de que la nueva Ley Orgánica no introduce novedades substanciales en este Capítulo.

mutatis mutandi, la ordenación jurídico-material recogida en la Ley española es idéntica a la que caracteriza la cuestión en el ámbito convencional y comunitario.

Lo que se pretende evitar en estos artículos es la deslocalización artificial del fichero por parte los operadores informáticos para eludir la aplicación de la ley española. Para ello, el juego combinado de los artículos 2 y 34 de la Ley Orgánica permite, de un lado, que en el ámbito nacional y comunitario, el responsable del tratamiento del fichero situado en España o en otro país comunitario, quede sometido a una legislación homogénea con el fin de evitar o prevenir la ilicitud de los tratamientos. Y de otro, que si el fichero está situado fuera del territorio español, se impida la transmisión de datos a países que no ofrezcan un adecuado nivel protección, y eventualmente que se les aplique la ley española si la recogida de datos fue hecha en España (art. 2 c).

Por último cabe hacer referencia a los trabajos La Conferencia de La Haya de DIPr., en la Mesa Redonda llevada a cabo en Ginebra. El grupo de expertos ha puesto de manifiesto que la "captura", tratamiento y transferencia de datos personales son inherentes al comercio electrónico. El estudio comparado de los diversos ordenamientos jurídicos pone de relieve que existen países en donde no hay regulación específica ni se exige un marco de reglamentación para el tratamiento de datos; en tanto que, otros países regulan de modo rígido tanto el tratamiento como la transferencia de datos personales. Es por ello que la determinación del derecho aplicable exige un estudio en profundidad de los diversos ordenamientos con el fin de articular una regulación uniforme mediante la cual se permita mayor intervención al juego de la autonomía de la voluntad en orden a la autoreglamentación de los intereses particulares, al tiempo que se favorezca la creación de contratos modelos. Sobre estos contratos modelo trabaja la CCI en base a los Principios contenidos en las recomendaciones de la OCDE (1980[40]), del Convenio del Consejo de Europa (1981[41]) y de los Principios de las Naciones Unidas (1990[42]).

A MODO DE CONCLUSIÓN

1. La "sociedad de servicios de la información" es una sociedad post-industrial construida sobre un sistema productivo basado en la automatización de las energías del hombre. En esta sociedad, la información y los servicios que la misma ofrece han pasado a ser una res intracommercium; esto es, un bien de consumo cuyo valor económico es muy elevado. Este fenómeno se incardina en un proceso virtual caracterizado por el hecho de que los bienes más preciados son bienes inmateriales los cuales se comercializan a través de un sistema de redes interconectadas que unen millones de ordenadores del mundo entero: Internet.

2. La regulación jurídica de los problemas que se plantean en esta sociedad de la información son de carácter pluridisciplinar, con matices complejos y perfiles diversos. Además, la posibilidad de violaciones masivas de derechos que afectan a la vida privada de los individuos y a los usuarios de los servicios de la información son aspectos que sólo pueden resolverse mediante la intervención directa de las administraciones públicas estatales y la colaboración internacional.

3. El Derecho internacional privado no es ajeno a estos problemas. Los mecanismos de reglamentación así como la rica y compleja técnica normativa de esta disciplina son cauces viables y válidos para dar respuestas a las nuevas cuestiones que se plantean en la sociedad de los servicios de la información. Ahora bien, los tradicionales puntos de conexión que propone el DIPr. se basan en gran medida en criterios territoriales no pensados para un espacio virtual

---

40 Recommendation du Conseil concernant les Lignes Directrices régissant la protection de la vie privée et les flux transfrontières des donnèes de caractère personal, de 23 de septiembre de 1980·

41 Convenio par la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España por Instrumento de 27 de enero de 1984 (BOE, de 15 de noviembre de 1985).

42 Comisión de Derechos Humanos, "Los derechos humanos y el progreso científico y tecnológico". Versión revisada de los Principios rectores para la reglamentación de los ficheros computerizados de datos de carácter personal. E/CN.4/1990/72, de 20 de febrero de 1990.

4. En el sector de los contratos los conflictos de leyes que pueden plantearse afectan a la concreción del derecho aplicable al contrato cuando los contratantes tienen su establecimiento en diversos países y el contrato se ha formalizado on-line. También se plantean problemas para la determinación de la ley aplicable a los derechos de autor, a la violación de tales derechos y a la precisión de la ley aplicable a la privacidad de los individuos. El potencial concurso de leyes de todos los Estados en donde se ha producido la carga o descarga del material, la conexión al Sitio, la recepción y difusión del material o el establecimiento del suministrador del servicio exigen la limitación y fijación de una única ley o de unas pocas leyes alternativas como garantía para la protección de los consumidores y usuarios. Es decir, garantizar la previsibilidad y la seguridad de este comercio electrónico.

5. Los tradicionales puntos de conexión de las normas conflictuales de DIPr. basados en criterios territoriales (ley del domicilio, de la residencia, del establecimiento, del lugar donde se produce el daño, del lugar donde se comete el ilícito, del lugar donde se realice la prestación característica, etc.), son viables y válidas para determinar el derecho aplicable incluso en un mundo virtual. Si bien es cierto que en el cyberespacio las partes no tienen "conciencia" del lugar físico en donde se encuentran respectivamente, ello no quiere decir que sus intereses carezcan de protección. No es imposible hallar una respuesta adecuada partiendo de la regulación existente. Que se puedan aplicar varias leyes no quiere decir que ello traiga consecuencias imposibles de resolver: estas situaciones son bien conocidas en el DIPr. Tampoco es nuevo para el DIPr., que un mismo acto pueda producir efectos en diferentes Estados y que en función de la calificación adoptada por la lex fori las respuestas puedan variar de un ordenamiento a otro.

6. Ante la ausencia en estos momentos de reglas convencionales sobre el uso de Internet que pudieran ayudar a eliminar los problemas del concurso de leyes aplicables teniendo en cuenta los aspectos particulares y las características tecnológicas del medio utilizado; y, ante las dificultades para la elaboración de unas reglas uniformes de derecho material aceptables por la comunidad internacional, es posible afirmar que el método conflictual sigue siendo válido y viable para que el legislador -nacional e internacional-, pueda buscar soluciones "de iure condendo" a los problemas y dificultades que en esta exposición hemos intentado poner de relieve.

REFERENCIA BIBLIOGRAFICA

Abarca Junco, P., "El derecho a la intimidad en el Derecho internacional privado español, *BFD* 2, UNED, 1993

— "Competencia judicial internacional en materia de difamación por artículos de prensa (a propósito de la sentencia del Tribunal de Justicia de 7 de marzo de 1995 (Fiona Shevill y otros c/ Presse Alliance, S.A.), en *Gaceta Jurídica de la CE*, B- 113 mayo 1996

Alvarez-Cienfuegos Suárez, J.Mª., "Las obligaciones concertadas por medios informáticos y la documentación electrónica de los actos jurídicos", *Informática y Derecho*, núm. 5, UNED-CRE, 1992

—"Documento electrónico", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* núm. 19-22 *(Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997)*, UNED-CRE, 1998

—"Implicaciones jurídicas de los sistemas electrónicos de comunicación", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* núm.. *19-22 (Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997)*, UNED-CRE, 1998

Alvarez Rico, M., "Informática y Derecho en España", *Informática y Derecho, (Revista Iberoamericana de Derecho Informático) núms. 23-26 (Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997)*, UNED-CRE, 1998

Barbry, E., "La responsabilité des prestataires d´hebergement sur l´Internet"; (con nota sobre la sentencia de la CA Paris, 14, ch, de 10 de febrero de 1999*), La Semaine Juridique*, núm 23 1999

Bariati, S., "Internet: Aspect rélatifs aux conflits de lois*", Riv.di diritto internazionale privato e processuale*, 1997-3

—"Internet e il diritto internazionale privato: aspetti relativi alla disciplina del diritto d´autore", *AIDA*, vol. 59, 1996

Barriuso Ruíz, C., *Contratación electrónica. Aspectos legales del comercio electrónico*, Dickynson, 1998

—"Contratación electrónica", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* núm. 19-22 *(Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997)*, UNED-CRE, 1998

Burnstein, M.R., "Conflicts on the Net: Choice of Law in Transnactional Cyberspace", *Vaderlbilt J.Transnat´l.L.*. vol.29, 1996

Cámara Lapuente, S., "El nuevo derecho *sui generis* sobre las bases de datos", *Actualidad Civil*, núm. 3/ 18-24 enero 1999

Caprioli, E.A. & **Sorieul**, R., "Le commerce international électronique: vers l´émergence de règles juridiques transnationales", *JDI*, abril-junio, 1997-2

Carrascosa González, J., "Circulación internacional de datos personales informatizados y la directiva 95/46/CE", *Actualidad Civil*, núm. 23/ 2-8 junio 1997

—"Contratos en el sector audiovisual e informático", en *Contratos Internacionales*, (A.L. Calvo Caravaca y L. Fernández de la Gándara, Dir), Tecnos, Madrid, 1997

Carrascosa López, V, Pozo Arranz, Mª.A y Rodríguez de Castro, E.P., *La contratación informática: el nuevo horizonte contractual*, Comares, Granada, 1997

—"Introducción a la contratación informática", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* núm 9-11, UNED-CRE, 1996

Cortés Margallo, B., "Informática y tecnologías de la información: breve síntesis de la evolución legislativa de la Unión Europea", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* núm. 23-26 *(Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997)*, UNED-CRE, 1998

Corredoira y Alfonso, L., "El derecho de acceso a la información en Internet", *Actualidad informática Aranzadi*, núm 32, julio 1999

Davara Rodríguez, M.A., (Dir), *X Años de encuentros sobre Informática y Derecho (1996-1997)*, U.Pontificia de Comillas, Aranzadi, 1997

— "Los principios de protección de datos y los derechos de las personas en la nueva Ley Orgánica de Protección de Datos de Carácter personal", en *Actualidad Informática Aranzadi*, núm. 34, enero 2000

Del Peso Navarro, E., "Principales diferencias entre la nueva Ley de Protección de Datos y la LORTAD", en *Actualidad Informática, Aranzadi*, núm. 34, enero 2000

Erdozáin López, J.C., "Ley de condiciones de Contratación: una perspectiva del comercio electrónico", El Foro, *Revista Otrosí*, Junio 1999

Espagnon, M., "Le paiement d´une somme d´argent sur Internet: évolution ou révolution du droit de moyens de paiement", *La Semaine Juridique*, núm. 16-17

Fernández López, J.M., "La nueva Ley de Protección de Datos de Carácter Personal de 13 de diciembre de 1999. Su por qué y sus principales novedades", en *Actualidad Informática Aranzadi*, núm. 34, enero 2000

Freixes Sanjuán, T., "La protección de los datos automatizados por el Tribunal Europeo de Derechos Humanos", en *Encuentros sobre Informática y Derecho 1997-1998*, (Coord. Davara Rodríguez, M.A.), Facultad del Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi, Pamplona, 1998

Gahtan, A., & Mann, F., "Legal Issues Relating to Internet Web Sites: A Canadian Perspective", *Cyberlaw Enciclopedia*, 1997 <http://www.gahtan.com/alan (page version, july, 1999)

Ginsburg, J.C., "The Private International Law of Cyberspace on an Erea of Technological Change", *RCA-DI*, vol. 273, 1998

González Ballesteros, T., "Libertad de expresión e Internet en el ámbito del Derecho", *Actualidad Informática Aranzadi*, núm. 32, julio 1999

Graf von Bernstorff, Ch., "Ausgewälte Rechtsprobleme im Electronic Commerce, en RIW, Heft 1/2000, pp. 14-20.

Guerra Balic, J.T., "La conclusión de contratos por medios informáticos", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)*, núm.8 UNED-CRE, 1995

Gutiérrez Sánchez, P., "Anteproyecto de la Ley Orgánica por la que se modifica la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD)", *Actualidad Informática Aranzadi*, núm. 28, julio 1998

Guzmán Zapater, M., "La protección de los consumidores en los contratos de venta negociados fuera de establecimiento mercantil (a propósito de la transposición de la Directiva CEE 85/577", en *Gaceta Jurídica de la CEE,* B-80, diciembre, 1992 y B-82, marzo 1993

Herrero-Tejedor, F., *Honor, Intimidad y Propia Imagen,* Colex, Madrid, 1994

Hicks, B.D., "Choice of Law Issues in Cybersapace", Texas Tech University, 1996 <http:// www.law.ttu.edu/cyberspace/jour13.htm>

Huet, J., "Quelle culture dans le "cyber-espace" et quels droits intellectuels pour cette cyber-culture?", *Recueil Dalloz,* ch. 18, 1998

Illescas Ortiz, R., "La firma electrónica y RDL 14/1999, de 17 de septiembre", en *Revista Derecho de los Negocios,* Octubre 1999

Jaccard,M., "Commerce électronique et droit d´auteur sur Internet", Rev. suisse de droit des affaires", núm. 70, 1998-2

Kessedjian, C., & **Kahn**. S., "Dispute Resolution On Line", *International Lawyer,* 1998

Legislación Informática (Datos personales, propiedad intelectual e industrial y titulaciones universitarias) (Eugenio Ull Pont, Coord), *UNED*-Madrid, 1997

Losano, M., *La informática y el análisis de los procesos jurídicos,* (trad. A. Elvira), Centro de Estudios Constitucionales, Madrid, 1991

Mankowski, P., "Das Internet im Internationalen Vertrags- und Delitsrecht", *RabelsZ Bd.* 63, 1999

Mazet, G., "Dimensiones internacionales de la informática jurídica documental", *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* núm. 8, UNED-CRE, 1995

Martínez Nadal. A., *Comercio electrónico, firma digital y autoridades de certificación,* Civitas, Madrid, 1998

—"Comercio electrónico", en *Curso sobre Protección Jurídica de los Consumidores, Civitas,* Madrid, 1999

—"Comentarios de urgencia al urgentemente aprobado RDL 14/1999, de 17 de septiembre, sobre firma electrónica", en *R.J. La Ley,* 1 y 2. 12.1999

Moreno Navarrete, M.A., *Contratos electrónicos,* Marcial Pons, Madrid, 1999

Orozco Pardo, G., "Responsabilidad civil en materia de informática", *Informática y Derecho, (Revista Iberoamericana de Derecho Informático) núms. 19-22 (Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997),* UNED-CRE, 1998

Perritt, H.H., "Jurisdiction in Cybersapce", 41, *Vill.L.Rev.*, 1-100, 1996

Prieto Gutiérrez, J.Mª, "La Directiva 95/46/CE como criterio unificador", *Informática y Derecho, (Revista Iberoamericana de Derecho Informático), núms. 23-26 (Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997),* UNED-CRE, 1998; *idem.*, "La Directiva 95/46/CE como criterio unificador", *en Poder Judicial,* núm. 48, 1997

Rodríguez de Castro, E., "Contratación Informática", *Informática y Derecho (Revista Iberoamericana de Derecho Informático),* núms. 19-22 *(Actas del Congreso "Marco Legal y Deontológico de la Informática", Mérida, 16-20 septiembre 1997),* UNED-CRE, 1998

Ribas Alejandro, J., *Aspectos jurídicos del comercio electrónico en Internet,* Aranzadi, Pamplona, 1999

—"Editorial Aranzadi gana el primer juicio en España por la comercialización ilegal de sus bases de datos por Internet", *Actualidad Jurídica Aranzadi,* núm 401, 29 julio 1999, p. 1 (el texto de la sentencia puede verse en *Actualidad informática Aranzadi,* núm. 32, julio 1999

Ruiz Miguel, C., "El derecho a la intimidad informática en el ordenamiento español", en *RGD,* vol. 607, abril, 1995

Swire, P.P., "Of Elephants, Mice, and Privacy: International Choice of Law and the *Internet*", *Int'l Law,* vol. 32, 1998

Trotter, H, "The Proper Legal Regime for 'cyberspace' ", *U.Pitt.L.Rev.*, 55,1994

Ustarán, A., "Aspectos legales de la actividad comercial en Internet", *R.J.La Ley,* 1997-5

Vargas Gómez-Urrutia, M., "Comercio Internacional Electrónico y Conflicto de Leyes y de Jurisdicciones en el *Cyberespacio", Revista Derecho de los Negocios,* Madrid, abril 2000

— "Recientes iniciativas y propuestas para la reglamentación del comercio electrónico", Revista Contratación electrónica, Sevilla, núm. 4, 2000

Vattier Fuenzalida, C., "En torno a los contratos electrónicos", *Revista General de Legislación y Jurisprudencia,* Tercera Epoca, enero-febrero 1999

Informe Nombres de Dominio

Erick Iriarte Ahon (Perú)
Red Científica Peruana.

INTRODUCCION

El presente informe esta destinado a presentar el panorama mundial sobre nombres de dominio y su problemática tanto política como jurídica vigente. Es fundamental para el análisis del presente documento los cuadros anexos en donde se presentan a los entes que participan directa e indirectamente en la toma de decisiones en temas de nombres de dominio.

La estructura de nombres de dominio tal como la conocemos ahora se basa en los documentos RFC 1031, 1032, 1033, 1034 y 1035, pero fundamentalmente en el documento de Postel denominado RFC 1591 (ver anexo 1).

Hasta la época en que se realiza el RFC 1591, el desarrollo de Internet estaba fundamentalmente centrado hacia las áreas académicas, pero para el año 1997 en el marco del denominado "Plan para el Comercio Electrónico Mundial", el gobierno de Bill Clinton dio la orden de privatizar el sistema de nombres de dominio. Es claro entonces que es el desarrollo exponencial del Internet, con la aparición de la web, que hace que los nombres de dominio sean parte importante en el proceso de desarrollo del Comercio Electrónico Mundial, lo que fundamenta la privatización del sistema de nombres de dominio.

"En consecuencia, el 2 de julio de 1997, el Departamento de Comercio emitió una Invitación a formular comentarios (Request for comments) (RFC) sobre la administración del DNS. La invitación a formular comentarios solicitaba la opinión pública sobre las cuestiones inherentes al marco global de la administración del DNS, la creación de nuevos dominios de nivel superior, las políticas relativas a los registradores de nombres de dominio, y las cuestiones relativas a las marcas. Durante el período correspondiente, se recibieron más de 430 comentarios, que totalizaron unas 1.500 páginas.

El 30 de enero de 1998, la Administración Nacional de Telecomunicaciones e Información (NTIA), una agencia del Departamento de Comercio, emitió Una Propuesta para Mejorar la Administración Técnica de los Nombres y Direcciones de Internet, a cuyo respecto se podían formular comentarios. La normativa propuesta, o "Libro Verde", se publicó en el Registro Federal, el 20 de febrero de 1998, dando al público la oportunidad de formular comentarios. Al cerrarse el período de recepción de los comentarios, el 23 de marzo de 1998, la NTIA había recibido más de 650 comentarios.

En el Libro Verde se propusieron ciertas medidas concebidas para privatizar la administración de los nombres y direcciones de Internet, de una manera que permita el desarrollo de una competencia fuerte y facilite la participación mundial en la administración de Internet. En el Libro Verde se sometieron a debate varias cuestiones relativas a la administración del DNS, incluida la creación por el sector privado de una nueva entidad sin fines de lucro (la "nueva entidad") administrada por una Junta de Directores que sea representativa tanto internacional como funcionalmente." (White Paper, departamento de Comercio de los Estados Unidos)

Tras los comentarios se presento la versión final del documento por parte del Departamento de Comercio de USA, dicho documento, que llevaba por título: "Administración de los nombres y direcciones de Internet", se denomino comúnmente "White Paper" (documento completo en español http://ecommerce.wipo.int/domains/process/esp/Whitepaper-es.html), en base al cual se solicita a la OMPI que prepare un informe sobre el registro de nombres de dominio (http://ecommerce.wipo.int/domains/process/esp/final_report.html) (ver resumen en el anexo 2), y en el mismo documento del Departamento de Comercio se establecen las bases para la constitución del Internet Corporation for Assigned Names and Numbers (ICANN) creada con el fin de administrar el Sistema de Nombres de Dominio de Internet.

ICANN

Fundamentalmente el ICANN presenta las siguientes funciones que eran parte en su casos del NSF anteriormente.

1) La asignación de direcciones numéricas a los usuarios de Internet.

Todos los ordenadores de Internet tienen un número único de IP. La IANA (http://www.iana.org/), *bajo la jefatura del Dr. Jon Postel, coordina este sistema mediante la asignación de lotes de direcciones numéricas a los registros regionales de IP (ARIN en América del Norte, RIPE en Europa, y APNIC en la región de Asia y el Pacífico), en virtud de contratos con el DARPA. A su vez, los mayores proveedores de servicios de Internet solicitan los lotes de direcciones de IP a registros regionales de IP. Entonces, los destinatarios de esos lotes de direcciones asignan nuevamente las direcciones a los proveedores más pequeños de servicios de Internet y a los usuarios finales. (White Paper, Departamento de Comercio).*

Cabe destacar actualmente que para Latinoamérica y el Caribe se esta planteando la creación del LACNIC (http://www.lacnic.org/), estructura tipo RIR, que tiene como planteamientos básicos:

El Registro Regional de Direcciones IP Latinoamericano y Caribeño (LACNIC), es la organización que administra el espacio de direcciones IP, Números de Sistemas Autónomos (ASN), resolución inversa y otros recursos para la región de América Latina y el Caribe (LAC) en nombre de la comunidad Internet.

Tiene como objetivos representar y promover los puntos de vista en el desarrollo de la región y colaborar en su crecimiento, además de promover oportunidades educacionales y políticas públicas.

Entre sus pautas LACNIC pretende ofrecer un servicio neutral, participativo, democrático y no lucrativo de calidad con un directorio elegido por sus miembros. En este contexto, la membresía se atendrá a reglas específicas, de acuerdo a la ubicación geográfica y al carácter de ISPs. Los miembros se regirán por un sistema de votación según el tamaño del espacio de direcciones que administren.

2) La administración del sistema de registro de nombres para los usuarios de Internet.

El espacio de nombres de dominio está construido como una jerarquía. Se divide en dominios de nivel superior (TLD) que, a su vez, están divididos en dominios de segundo nivel (SLD), y así sucesivamente. Más de 200 TLD nacionales, o de código de país (country-code) (ccTLD), son administrados por sus gobiernos correspondientes o por entidades privadas, con la conformidad del gobierno nacional pertinente. Un pequeño conjunto de gTLD no llevan identificador nacional alguno, pero denotan la función prevista para esa porción del espacio de dominio. Por ejemplo, .com se estableció para los usuarios comerciales, .org para las organizaciones sin fines de lucro, y .net para los proveedores de servicios de red. En virtud de un acuerdo quinquenal de cooperación con la NSF, la se encarga del registro y la difusión de esos gTLD clave. Este acuerdo caduca el 30 de septiembre de 1998. (White Paper, Departamento de Comercio de USA).

En esta función específica es donde más se ha desarrollado el ICANN, teniendo ahora que el acuerdo establecido con NSI para el registro y difusión de nombres de dominio, ha entrado a una estructura "de mercado" que tiene unas 30 instituciones actualmente funcionando para este nivel, cabe destacar que no se presentan instituciones para gTLD en latinoamérica. (Ver anexo 3).

El ICANN posee un Board, que es actualmente el que lo dirige y coordina las acciones que efectua el ICANN (http://www.icann.org/general/abouticann.htm). Los miembros del Board son: Esther Dyson (Chairman), Jean-François Abramatic, Amadeu Abril i Abril, Robert Blokzijl, Geraldine Capdeboscq, Vinton G. Cerf , Jonathan Cohen, George Conrades, Greg Crew, Philip Davidson, Frank Fitzsimmons, Ken Fockler, Hans Kraaijenbrink, Jun Murai, Alejandro Pisanty, Michael Roberts, Eugenio Triana, Linda S. Wilson yPindar Wong. La participación Latinoamérica

en el board esta dada por Alejandro Pisanty, propuesto por Enred en las últimas elecciones, Pisanty trabaja en el NIC-MX y es un destacado propulsor del Internet en su país.

La estructura del ICANN esta basada en las llamadas Suporting Organizations, que pueden estar integradas a alguna de las siguientes partes:

1. The Address Supporting Organization (ASO) relacionada a lo concerniente a los números IP.

2. The Domain Name Supporting Organization (DNSO), que esta relacionada al sistema de nombres de dominio, estructura que permite un camino-fácil-de-recordar para los números IP.

3. The Protocol Supporting Organization (PSO), es la estructura más técnica dentro del ICANN, y se dedica a los protocolos, standares técnicos para intercambio de información y sobre todo al manejo de la comunicación por medio de Internet.

Como indicamos líneas arriba el registro de número IP en latinoamérica (donde nos encontramos) depende de ARIN, pero se esta solicitando que pase al LACNIC, con lo cual esta sería la forma de participación directa en la ASO (http://www.aso.icann.org/). Actualmente la ASO posee 9 miembros, ninguno de latinoamérica. Son 3 del APNIC (Asia-Pacífico), 3 de ARIN (América (entiendase Norte-América)) y 3 de RIPE NCC (Europa).

El PSO, es un organismo altamente técnico, creado en Abril de 1999, y refrendado en la reunión de Santiago de Chile de Agosto de 1999. Sus actuales miembros son:

Steve Bellovin - IETF (Internet Engineering Task Force) (http://www.ietf.org)
Fabio Bigi - ITU (International Telecommunications Union) (http://www.itu.int)
Leslie Daigle - IETF (Internet Engineering Task Force)
Philipp Hoschka - W3C (World Wide Web Consortium) (http://www.w3.org/)
Bridget Cosgrave - ETSI (European Telecommunications Standards Institute)
Gerry Lawrence - ETSI (http://www.etsi.org/)
Brian Moore - ITU (International Telecommunications Union)
Daniel Weitzner - W3C (World Wide Web Consortium)

Finalmente el DNSO, es el grupo que mayor interes y participación requiere. Dado que el tema de los números IP es en si muy técnico es en el DNSO donde se ven la mayoría de los problemas políticos, jurídicos y económicos relacionados con los nombres de dominio. Ciertamente que si bien el ICANN solo ve nombres de dominio y número IP, ya se han comenzado a establecer los primeros grupos de trabajo que estan analizando e-commerce en su relación con nombres de dominio, entre otros temas, por lo cual consideramos que la participación dentro de los diversos grupos es fundamental.

La DNSO (http://www.dnso.icann.org/), presenta los siguientes grupos:

- ccTLD registries. This constituency consists of managers of country-code (i.e. two-letter) top-level domains.

- Commercial and business entities. This constituency represents the views and interests of those stakeholders who use the Internet to conduct their business or part of it.

- gTLD registries. This constituency consists of present operators of gTLD registries. Its only current member is Network Solutions, Inc.

- ISP and connectivity providers. The ISPCP constituency represents entities that are in the business of operating DNS nameservers as a service for third parties and that either operate an Internet backbone network based on TCP/IP or provide transit either to Internet users or to third parties' Internet content.

- Non-commercial domain name holders. The NCDNHC consists of organizations (a) holding at least one domain name (b) that are incorporated as a non-commercial entity or, if not incorporated, that operate on a not-for-profit basis primarily for non-commercial purposes and (c) that are engaged in activities that are primarily non-commercial, including, e.g., political, educational, religious, charitable, scientific and artistic.

- Registrars. This constituency is currently made up of members who meet the requirements for being an ICANN-accredited registrar. The intention in the future is to broaden the focus to include ccTLD registrars, and perhaps resellers and those performing services and operations like a "registrar."

- Trademark, other intellectual property and anti-counterfeiting interests (IPC). The IPC represents the views and interests of users of intellectual property world-wide with particular emphasis on trademark, copyright, and related intellectual property rights and their effect and interaction with the DNS.

Hay que agregar que a las diversas entidades integrantes del DNSO, se agregan los siguientes grupos de trabajo permanentes:

Working Group B - Famous Trade-Marks
Working Group C - New gTLDs
Working Group D - Business Plan and Internal Procedures
Working Group E - Global Awareness and Outreach

Es de especial intéres actualmente el informe del grupo C de trabajo (http://www.dnso.org/dnso/notes/20000321.NCwgc-report.html) que presenta la necesidad de creación de nuevos dominios del tipo gTLD, dicho documento ya había sido presentado en la reunión del Cairo, a inicios de marzo del 2000, este informe ha tenido varios puntos de diferencia sobre todo entre los grupos non-commercial y los grupos commercial, puesto que en el registro se plantea como base el documento del grupo B de trabajo (http://www.dnso.org/dnso/notes/20000321.NCwgb-report.html), dicho documento (Grupo B), indica que las marcas famosas deben tener prioridad sobre otras para el registro. Esta situación tiene dos problemas sobre todo que los términos Trademark, Copyright y Famous Trademark, no tienen traducción literal al español y dependiendo el país tienen significaciones distintas, es decir al basarse en el derecho del common-law se estarían originando diversos problemas a los países que utilizan el roman-law como base jurídica (casi toda latinámerica y europa). El segundo punto en conflicto, es quien tendría el mejor derecho para la tener un nombre de dominio, sobre todo con la creación de nuevos gTLD que evitarían problemas.

GOVERNMENTAL ADVISORY COMMITTEE (GAC)

Este organismo de asesoramiento del ICANN, esta definido por la ByLaws del ICANN en el siguiente artículo:

The ICANN Bylaws (Article VII, Section 3(b)) describe the Governmental Advisory Committee as follows:

There shall be a Governmental Advisory Committee. The initial chairman of the Governmental Advisory Committee shall be appointed by the Board and shall hold that position until the election of his or her successor; subsequent chairs shall be elected by the members of the Governmental Advisory Committee pursuant to procedures adopted by such members. Membership of the Governmental Advisory Committee shall be open to all national governments. Membership shall also be open to Distinct Economies as recognized in international fora, and multinational governmental organizations and treaty organizations, on the invitation of the Governmental Advisory Committee through its Chair, or on invitation of the ICANN Board. Members of the Governmental Advisory Committee shall appoint one accredited representative to the Committee. The accredited representative of a member must hold a formal official position with the member's public administration. The term "official" includes a holder of an elected governmental office, or a person who is employed by such government, public authority or multina-

tional governmental or treaty organization and whose primary function with such government, public authority or organization is to develop or influence governmental or public policies. The Governmental Advisory Committee should consider and provide advice on the activities of the Corporation as they relate to concerns of governments, particularly matters where there may be an interaction between the Corporation's policies and various laws, and international agreements. The Board will notify the chairman of the Governmental Advisory Committee of any proposal for which it seeks comments under Article III, Section 3(b) and will consider any response to that notification prior to taking action.

Actualmente el coordinador y chairman del GAC es: Paul Twomey, quien actualmente se desempeña como Executive General Manager positions with the Australian Trade Commission (Austrade).

El representante peruano ante el GAC es: Carlos Valdez, Jefe de la Unidad Especial de Conseciones en Telecomunicaciones, Ministerio de Transportes (cavaldez@mtc.gob.pe), aunque el mismo no asistiera a las tres últimas reuniones del GAC, siendo representado en Santiago de Chile por Luis Cipriano (quien no llego a participar en ninguna reunión por llegar fuera de fecha), por un representante de la embajada peruana en la reunión de Los Angeles, y finalmente representado por un funcionario de la embajada del Perú en Egipto, en la reunión del Cairo.

Cabe destacar que en la reunión del Cairo (ver anexo 4), el GAC presento el siguiente documento: Principles for the Delegaltion and Administratio of Country Code Top Level Domains (http://www.noie.gov.au/gac/ccdocs/cctld.txt). El mismo que requiere ser analizado puntualmente sobre todo por los ccTLD que no son dependencias del Estado, puesto que el GAC declara la intención de la soberanía sobre los nombres de dominio, con lo cual se alterarían muchos de los esquemas actuales sobre registro de nombres de dominio, en especial el caso del PE-NIC y de muchos de las entidades de registro de ccTLD en latinoamérica, tienen que ser analizados.

Asimismo hay que destacar la posición del GAC sobre la UDRP (http://www.icann.org/udrp/udrp.htm), es decir sobre las técnicas de resolución de conflictos de nombres de dominio, que actualmente esta en plena vigencia.

PE-NIC

El registro de nombres de dominio para el cc .PE corresponde al PE-NIC (http://www.nic.pe), que se encuentra relacionado a la Red Científica Peruana.

Las políticas actuales del PENIC estan basadas en el documento Postel y en las políticas que estableciera Red Iris, para el country code .ES, hacia el año 1996., Actualmente las políticas del .ES han pasado a manos del Ministerio de Fomento, actualizandose y modernizandose.

Algunas políticias que podrían utilizarse en el PENIC paara mejorar su competitividad pueden ser: una apertura para suscripción de más de un nombre de dominio, tal como se tenía establecido hasta ahora. Asimismo se permitirá el registro por parte de personas naturales de nombres de dominio, con lo cual se espera que el número actual de nombres de dominio registrados aumente sustancialmente. Asimismo convertirá al .PE en un dominio competitivo con referencia a otros dominios.

Otro tema de cambio estaría dado por la resolución de conflictos, para lo cual se ha llegado a un acuerdo con el Cibertribunal Peruano (http://www.cibertribunalperuano.org), entidad de arbitraje especializada en temas de derecho informático, para la resolución de los conflictos existentes para registro de nombres de dominio .PE, la base normativa sera la UDRP y supletoriamente las normas jurídicas vigentes en el Perú.

ANEXO 1: DOCUMENTO POSTEL

Network Working Group — J. Postel
Request for Comments: 1591 — ISI
Category: Informational — March 1994

Domain Name System Structure and Delegation

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

1. Introduction

This memo provides some information on the structure of the names in the Domain Name System (DNS), specifically the top-level domain names; and on the administration of domains. The Internet Assigned Numbers Authority (IANA) is the overall authority for the IP Addresses, the Domain Names, and many other parameters, used in the Internet. The day-to-day responsibility for the assignment of IP Addresses, Autonomous System Numbers, and most top and second level Domain Names are handled by the Internet Registry (IR) and regional registries.

2. The Top Level Structure of the Domain Names

In the Domain Name System (DNS) naming of computers there is a hierarchy of names. The root of system is unnamed. There are a set of what are called "top-level domain names" (TLDs). These are the generic TLDs (EDU, COM, NET, ORG, GOV, MIL, and INT), and the two letter country codes from ISO-3166. It is extremely unlikely that any other TLDs will be created.

Under each TLD may be created a hierarchy of names. Generally, under the generic TLDs the structure is very flat. That is, many organizations are registered directly under the TLD, and any further structure is up to the individual organizations.

In the country TLDs, there is a wide variation in the structure, in some countries the structure is very flat, in others there is substantial structural organization. In some country domains the second levels are generic categories (such as, AC, CO, GO, and RE), in others they are based on political geography, and in still others, organization names are listed directly under the country code. The organization for the US country domain is described in RFC 1480 [1].

Each of the generic TLDs was created for a general category of organizations. The country code domains (for example, FR, NL, KR, US) are each organized by an administrator for that country. These administrators may further delegate the management of portions of the naming tree. These administrators are performing a public service on behalf of the Internet community. Descriptions of the generic domains and the US country domain follow.

Of these generic domains, five are international in nature, and two are restricted to use by entities in the United States.

World Wide Generic Domains:

COM - This domain is intended for commercial entities, that is companies. This domain has grown very large and there is concern about the administrative load and system performance if the current growth pattern is continued. Consideration is being taken to subdivide the COM domain and only allow future commercial registrations in the subdomains.

EDU - This domain was originally intended for all educational institutions. Many Universities, colleges, schools, educational service organizations, and educational consortia have registered here. More recently a decision has been taken to limit further registrations to 4 year colleges and universities. Schools and 2-year colleges will be registered in the country domains (see US Domain, especially K12 and CC, below).

NET - This domain is intended to hold only the computers of network providers, that is the NIC and NOC computers, the administrative computers, and the network node computers. The customers of the network provider would have domain names of their own (not in the NET TLD).

ORG - This domain is intended as the miscellaneous TLD for organizations that didn't fit anywhere else. Some non- government organizations may fit here.

INT - This domain is for organizations established by international treaties, or international databases.

United States Only Generic Domains:

GOV - This domain was originally intended for any kind of government office or agency. More recently a decision was taken to register only agencies of the US Federal government in this domain. State and local agencies are registered in the country

domains (see US Domain, below).

MIL - This domain is used by the US military.

Example country code Domain:

US - As an example of a country domain, the US domain provides for the registration of all kinds of entities in the United States on the basis of political geography, that is, a hierarchy of <entity-name>.<locality>.<state-code>.US. For example, "IBM.Armonk.NY.US". In addition, branches of the US domain are provided within each state for schools (K12), community colleges (CC), technical schools (TEC), state government agencies (STATE), councils of governments (COG),libraries (LIB), museums (MUS), and several other generic types of entities (see RFC 1480 for details [1]).

To find a contact for a TLD use the "whois" program to access the database on the host rs.internic.net. Append "-dom" to the name of TLD you are interested in. For example:

whois -h rs.internic.net us-dom
or
whois -h rs.internic.net edu-dom

3. *The Administration of Delegated Domains*

The Internet Assigned Numbers Authority (IANA) is responsible for the overall coordination and management of the Domain Name System (DNS), and especially the delegation of portions of the name space called top-level domains. Most of these top-level domains are two-letter country codes taken from the ISO standard 3166.

A central Internet Registry (IR) has been selected and designated to handled the bulk of the day-to-day administration of the Domain Name System. Applications for new top-level domains (for example, country code domains) are handled by the IR with consultation with the IANA. The central IR is INTERNIC.NET. Second level domains in COM, EDU, ORG, NET, and GOV are registered by the Internet Registry at the InterNIC. The second level domains in the MIL are registered by the DDN registry at NIC.DDN.MIL. Second level names in INT are registered by the PVM at ISI.EDU.

While all requests for new top-level domains must be sent to the Internic (at hostmaster@internic.net), the regional registries are often enlisted to assist in the administration of the DNS, especially in solving problems with a country administration. Currently, the RIPE NCC is the regional registry for Europe and the APNIC is the

regional registry for the Asia-Pacific region, while the INTERNIC administers the North America region, and all the as yet undelegated regions.

The contact mailboxes for these regional registries are:

INTERNIC hostmaster@internic.net
APNIC hostmaster@apnic.net
RIPE NCC ncc@ripe.net

The policy concerns involved when a new top-level domain is established are described in the following. Also mentioned are concerns raised when it is necessary to change the delegation of an established domain from one party to another.

A new top-level domain is usually created and its management delegated to a "designated manager" all at once.

Most of these same concerns are relevant when a sub-domain is delegated and in general the principles described here apply recursively to all delegations of the Internet DNS name space.

The major concern in selecting a designated manager for a domain is that it be able to carry out the necessary responsibilities, and have the ability to do a equitable, just, honest, and competent job.

1) The key requirement is that for each domain there be a designated manager for supervising that domain's name space. In the case of top-level domains that are country codes this means that there is a manager that supervises the domain names and operates the domain name system in that country.

The manager must, of course, be on the Internet. There must be Internet Protocol (IP) connectivity to the nameservers and email connectivity to the management and staff of the manager.

There must be an administrative contact and a technical contact for each domain. For top-level domains that are country codes at least the administrative contact must reside in the country involved.

2) These designated authorities are trustees for the delegated domain, and have a duty to serve the community.

The designated manager is the trustee of the top-level domain for both the nation, in the case of a country code, and the global Internet community.

Concerns about "rights" and "ownership" of domains are inappropriate. It is appropriate to be concerned about "responsibilities" and "service" to the community.

3) The designated manager must be equitable to all groups in the domain that request domain names.

This means that the same rules are applied to all requests, all requests must be processed in a non-discriminatory fashion, and academic and commercial (and other) users are treated on an equal basis. No bias shall be shown regarding requests that may come from customers of some other business related to the manager — e.g., no preferential service for customers of a particular data network provider. There can be no requirement that a particular mail system (or other application), protocol, or product be used.

There are no requirements on subdomains of top-level domains beyond the requirements on higher-level domains themselves. That is, the requirements in this memo are applied recursively. In particular, all subdomains shall be allowed to operate their own domain name servers, providing in them whatever information the

subdomain manager sees fit (as long as it is true and correct).

4) Significantly interested parties in the domain should agree that the designated manager is the appropriate party.

The IANA tries to have any contending parties reach agreement among themselves, and generally takes no action to change things unless all the contending parties agree; only in cases where the designated manager has substantially mis-behaved would the IANA step in.

However, it is also appropriate for interested parties to have some voice in selecting the designated manager.

There are two cases where the IANA and the central IR may establish a new top-level domain and delegate only a portion of it: (1) there are contending parties that cannot agree, or (2) the applying party may not be able to represent or serve the whole country. The later case sometimes arises when a party outside a country is trying to be helpful in getting networking started in a country — this is sometimes called a "proxy" DNS service.

The Internet DNS Names Review Board (IDNB), a committee established by the IANA, will act as a review panel for cases in which the parties can not reach agreement among themselves. The IDNB's decisions will be binding.

5) The designated manager must do a satisfactory job of operating the DNS service for the domain.

That is, the actual management of the assigning of domain names, delegating subdomains and operating nameservers must be done with technical competence. This includes keeping the central IR (in the case of top-level domains) or other higher-level domain manager advised of the status of the domain, responding to requests in a timely manner, and operating the database with accuracy, robustness, and resilience.

There must be a primary and a secondary nameserver that have IP connectivity to the Internet and can be easily checked for operational status and database accuracy by the IR and the IANA.

In cases when there are persistent problems with the proper operation of a domain, the delegation may be revoked, and possibly delegated to another designated manager.

6) For any transfer of the designated manager trusteeship from one

organization to another, the higher-level domain manager (the IANA in the case of top-level domains) must receive communications from both the old organization and the new organization that assure the IANA that the transfer in mutually agreed, and that the new organization understands its responsibilities.

It is also very helpful for the IANA to receive communications from other parties that may be concerned or affected by the transfer.

4. Rights to Names

1) Names and Trademarks

In case of a dispute between domain name registrants as to the rights to a particular name, the registration authority shall have no role or responsibility other than to provide the contact information to both parties.

The registration of a domain name does not have any Trademark status. It is up to the requestor to be sure he is not violating anyone else's Trademark.

2) Country Codes

The IANA is not in the business of deciding what is and what is not a country.

Postel [Page 6]

RFC 1591 Domain Name System Structure and Delegation March 1994

The selection of the ISO 3166 list as a basis for country code top-level domain names was made with the knowledge that ISO has a procedure for determining which entities should be and should not be on that list.

5. Security Considerations

Security issues are not discussed in this memo.

6. Acknowledgements

Many people have made comments on draft version of these descriptions and procedures. Steve Goldstein and John Klensin have been particularly helpful.

7. Author's Address

Jon Postel
USC/Information Sciences Institute

4676 Admiralty Way
Marina del Rey, CA 90292

Phone: 310-822-1511
Fax: 310-823-6714
EMail: Postel@ISI.EDU

7. References

[1] Cooper, A., and J. Postel, "The US Domain", RFC 1480, USC/Information Sciences Institute, June 1993.

[2] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1340, USC/Information Sciences Institute, July 1992.

[3] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, USC/Information Sciences Institute, November 1987.

[4] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, USC/Information Sciences Institute, November 1987.

[6] Partridge, C., "Mail Routing and the Domain System", STD 14, RFC 974, CSNET CIC BBN, January 1986.

[7] Braden, R., Editor, "Requirements for Internet Hosts — Application and Support", STD 3, RFC 1123, Internet Engineering Task Force, October 1989.

ANEXO 2: RESUMEN DEL INFORME WIPO SOBRE NOMBRES DE DOMINIO

RESUMEN

Los nombres de dominio son las direcciones de Internet expresadas simplemente para facilidad del usuario. Si bien fueron diseñados con el fin de permitir a los usuarios localizar ordenadores de manera fácil, los nombres de dominio han adquirido mayor importancia en tanto que indicadores comerciales y, como tales, han provocado conflictos con el sistema de identificadores comerciales que existía antes de la llegada de Internet y que está protegido por derechos de propiedad intelectual.

La tensión que existe entre los nombres de dominio, por una parte, y los derechos de propiedad intelectual, por otra, ha provocado numerosos problemas que plantean interesantes cuestiones de política. Estas cuestiones de política tienen nuevas dimensiones que son consecuencia de la intersección de un medio mundial con propósitos múltiples, como es Internet, con sistemas diseñados para el mundo territorial y físico.

Como consecuencia de la propuesta del Gobierno de los Estados Unidos de América, y con la aprobación de sus Estados miembros, la OMPI ha emprendido, desde julio de 1998, un amplio proceso internacional de consultas ("Proceso de la OMPI"). El objetivo del Proceso de la OMPI consiste en formular recomendaciones a la entidad

creada para administrar el sistema de los nombres de dominio, la Corporación de Asignación de Nombres y Números de Internet (ICANN), en relación con ciertas cuestiones derivadas de la interfaz entre los nombres de dominio y los derechos de propiedad intelectual. Durante el Proceso de la OMPI, se han celebrado 17 consultas en 15 ciudades diferentes en todo el mundo y se han recibido informes escritos de 344 gobiernos, organizaciones intergubernamentales, asociaciones profesionales, corporaciones y personas individuales.

Como parte del Proceso de la OMPI, en diciembre de 1998 se publicó un Informe provisional en el que figura el proyecto de recomendaciones. El presente documento constituye el Informe final, que se ha presentado a la ICANN y a los Estados miembros de la OMPI. Las principales recomendaciones del Informe final se resumen a continuación.

Las mejores prácticas para los órganos de registro

i) La adopción de varias prácticas normativas perfeccionadas para los funcionarios encargados de los registros con potestad para registrar nombres de dominio en los dominios de nivel superior genéricos (gTLD) reducirá la tensión que existe entre los nombres de dominio y los derechos de propiedad intelectual.

ii) En particular, la compilación y disponibilidad de datos de contacto fiables y exactos sobre los titulares de nombres de dominio constituye un instrumento esencial para facilitar la protección de los derechos de propiedad intelectual en un medio anónimo e ilimitado. Dichos datos de contacto proporcionan los medios principales para que los titulares de propiedad intelectual puedan seguir el proceso que les permitirá hacer valer sus derechos.

iii) Cuando se establezca que los datos de contacto son inexactos y poco fiables y que no se puede establecer por su conducto el contacto con el titular de un nombre de dominio, una tercera parte podrá presentar una notificación a este respecto al registrador responsable. Si se verifica de manera independiente la imposibilidad de establecer el contacto, podrá solicitarse al registrador que cancele el registro del nombre de dominio.

iv) En el Informe provisional de la OMPI se sugería que se examinase la introducción de un dominio no comercial, de uso restringido, en el que los datos de contacto de los titulares de nombres de dominio no estuvieran a disposición del público, a fin de disipar las preocupaciones de quienes consideran que la disponibilidad pública de los datos de contacto puede favorecer intromisiones en la vida privada. En el Informe final, se concluye que esta idea necesita seguir siendo ponderada, elaborada y consultada en un proceso separado antes de que puedan formularse recomendaciones al respecto.

Procedimiento administrativo relativo al registro abusivo de los nombres de dominio

v La ICANN debería aprobar una política de solución de controversias en virtud de la cual se ofreciese un procedimiento administrativo de solución de controversias para los conflictos relativos a los nombres de dominio en todos los gTLD. En el Informe provisional se recomendaba que se exigiese a los solicitantes de nombres de dominio someterse al procedimiento en relación con cualquier conflicto de propiedad intelectual que se plantease en relación con la inscripción de un nombre de dominio. El Informe final recomienda que se limite el alcance del procedimiento administrativo a los casos de mala fe, registro abusivo de nombres de dominio que infrinjan derechos de marcas ("ciberocupación", en términos populares). Así pues, se exigirá a los titulares de nombres de dominio que se sometan al procedimiento administrativo únicamente a raíz de denuncias relativas a la ciberocupación, que fue condenada universalmente en el Proceso de la OMPI como una actividad inexcusable, que debería ser suprimida.

vi) El procedimiento administrativo será rápido, eficaz, rentable y se realizará, en gran medida, en línea. Las decisiones que se tomen en virtud de este procedimiento se limitarán a ordenar la anulación o la transferencia de registros de nombres de dominio y la atribución de los costos del procedimiento (excluidos los honorarios de los abogados) a la parte perdedora. Los órganos de registro harán respetar las decisiones en virtud de la política de solución de controversias.

Exclusión para las marcas famosas y notoriamente conocidas

vii) Las marcas famosas y notoriamente conocidas han sido el objetivo especial de prácticas predatorias y parasitarias por parte de una minoría pequeña pero activa de solicitantes de registro. Debería introducirse un mecanismo por el cual el titular de una marca famosa o notoriamente conocida pueda obtener la exclusión en algunos o todos los gTLD del nombre de la marca, allí donde la marca sea famosa o notoriamente conocida con amplia base geográfica y en relación con distintas clases de bienes o servicios. El efecto de la exclusión consistiría en impedir que toda persona distinta del titular de la marca famosa o notoriamente conocida pueda registrar la marca como nombre de dominio.

viii El mecanismo de exclusión refleja en el espacio cibernético la protección especial establecida para las marcas famosas y notoriamente conocidas en el Convenio de París para la Protección de la Propiedad Industrial y en el Acuerdo sobre los ADPIC.

ix) Puesto que una exclusión abarcaría únicamente el nombre exacto de la marca famosa o notoriamente conocida y puesto que la experiencia muestra que los ciberocupadores suelen registrar numerosas variaciones similares de marcas famosas o notoriamente conocidas, la exclusión, una vez concedida, debería constituir una presunción probatoria en el procedimiento administrativo. El efecto de la presunción probatoria consistiría en que la responsabilidad de presentar justificación para la utilización de un nombre de dominio incumbiese al titular del nombre de dominio cuando el nombre de dominio sea idéntico o engañosamente similar a la marca famosa o notoriamente conocida y el nombre de dominio se utilice de manera que pueda perjudicar a los intereses del titular de la marca.

Nuevos gTLD

x) Las pruebas indican que la experiencia de los últimos cinco años en los gTLD ha conducido a numerosos casos de registro abusivos de nombres de dominio y ha provocado, en consecuencia, la confusión del consumidor y ha mermado la confianza que merece Internet al público. Ha conducido asimismo a la necesidad de que los titulares de propiedad intelectual inviertan sustanciales recursos humanos y financieros en la defensa de sus intereses. Esta discutible y antieconómica desviación de los recursos puede evitarse mediante la adopción de las prácticas de registro mejoradas, el procedimiento administrativo de solución de controversias y el mecanismo de exclusión que se recomiendan en el Informe final del Proceso de la OMPI.

xi) A la luz de la experiencia pasada, los titulares de propiedad intelectual se muestran sumamente aprensivos a introducir nuevos gTLD y a que pueda repetirse dicha experiencia en los nuevos gTLD.

xii) En la formulación de una política relativa a la introducción de nuevos gTLD intervienen muchas cuestiones, además de la protección de la propiedad intelectual. En lo tocante a la propiedad intelectual, se cree que puede tomarse en consideración la introducción de nuevos gTLD, a condición de que se aprueben las recomendaciones contenidas en el Informe final de la OMPI en relación con las prácticas de registro mejoradas, la solución de controversias y un mecanismo de exclusión

para las marcas famosas y notoriamente conocidas y a condición asimismo de que los nuevos gTLD se introduzcan de manera lenta y controlada, a fin de que pueda controlarse y evaluarse la experiencia con los nuevos gTLD.

Primeras medidas y cuestiones importantes

Las recomendaciones contenidas en el Informe final del Proceso de la OMPI han sido destinadas a los problemas mayores que existen entre la propiedad intelectual y los nombres de dominio y a obtener soluciones eficaces para dichos problemas. Ahora bien, siguen existiendo otras cuestiones importantes que requieren mayor reflexión y consulta. Entre estas cuestiones se encuentran:

a) como ya se ha señalado anteriormente, la exploración de la viabilidad de introducir un dominio no comercial, de uso restringido en el que no se pongan a disposición del público los datos de contacto de los titulares de nombres de dominio;

b) el problema de la mala fe, el registro abusivo de nombres de dominio que infringe los derechos de propiedad intelectual distintos de las marcas registradas o marca de productos, por ejemplo, indicaciones geográficas y derechos de la personalidad;

c) el problema de la mala fe, el registro abusivo, en tanto que nombres de dominio, de los nombres y siglas de organizaciones intergubernamentales internacionales que están protegidas por el Convenio de París contra su utilización y registro como marcas; y

d) el problema de la mala fe, el registro abusivo, en tanto que nombres de dominio, de las denominaciones comunes internacionales seleccionadas por la Organización Mundial de la Salud para identificar sustancias farmacéuticas específicas mediante nombres únicos y mundialmente disponibles, a fin de proteger la salud de los pacientes.

ANEXO 3 : LIST OF ACCREDITED AND ACCREDITATION-QUALIFIED REGISTRARS

Companies accredited, and currently operational, as registrars:

A+Net/ABACUS America, Inc. (United States)
Alabanza, Inc. d/b/a Bulkregister (United States)
All West Communications (United States)
America Online (United States)
CORE - Council of Internet Registrars (Switzerland)
Domain Bank, Inc. (United States)
Domain Direct (Canada)
domaininfo.com (Sweden)
DomainPeople (Canada)
Domain Registration Services (United States)
Dotster, Inc. (United States)
Easyspace Ltd. (United Kingdom)
eNom, Inc. (United States)
France Telecom/Oléane (France)
GANDI (France)
HANGANG Systems Inc. (Republic of Korea)
InterAccess Company (United States)
Internet Domain Registrars (Canada & United States)
interQ Incorporated (Japan)

Marvin Enterprises, Inc./Global Knowledge Group (United States)
Melbourne IT (Australia)
The NameIt Corporation (United States)
NameSecure.com (United States)
Network Solutions (United States)
Nominalia (Spain)
NORDNET (France)
PSI-Japan (Japan)
register.com (United States)
Signature Domains, Inc. (United States)
TierraNet Inc. (United States)

Companies accredited, but not yet operational, as registrars:

#1 Domain Names International (United States)
7WAYS (France)
A Technology Company (Canada)
Active ISP (Norway)
Affinity Hosting, LLC (United States)
American Domain Name Registry (United States)
Animus Communications, Inc. (United States)
CADVision d/b/a GetDomain.com (Canada)
Capital Networks Pty Ltd. (Australia)
CASDNS, Inc. (United States)
Catalog.com Inc. (United States)
CommuniTech.net, Inc. (United States)
Computer Data Networks (Kuwait)
Concentric Network Corp. (United States)
CSL Computer Service Langenbach GmbH (Germany)
Cydian Technologies (United States)
DADA SRL (Italy)
DomainRegistry.com (United States)
DomainZoo.com, Inc. (United States)
Eastern Communications Co., Ltd. (China)
EnetRegistry.com Corporation (United States)
EPAG Enter-Price Multimedia AG (Germany)
ExtremeNames.com (United States)
FreeYellow.Com (United States)
IBI Company Ltd. (Republic of Korea)
iDirections, Inc. (United States)
iHoldings.com Inc. d/b/a DotRegistrar.com (Untied States)
InfoAvenue (United States)
InfoNetworks (United Kingdom/United States)
infoUSA.com, Inc. (United States)
Interactive Telecom Network (United States)
Internet Domain Registry (Israel)
Internet Fr SA (France)
InterNeXt, Inc. (France)
iTool.com (United States)
MS Intergate (United States)
NamesDirect.com (United States)

NameEngine Inc. (United States)
Name.Space Inc. (United States)
NetBenefit (United Kingdom)
OnlineNIC, Inc. (China)
ProBoard Technologies (United States)
PSI-USA (United States)
PSINet, Inc. (United States & global)
Research Institute for Computer Science, Inc. (Japan)
Schlund + Partner AG (Germany)
Secura Company (Germany)
Shaver Communications Inc. (United States)
SiteName (Israel)
Speednames, Inc. (United States, Denmark, Singapore, Sweden)
Stargate Communications, Inc. (United States)
Talk.Com, Inc. (United States)
TechDogs (United States)
The Direct Connection Ltd. (United Kingdom)
TotalWeb Solutions (United Kingdom)
Virtual Internet (United Kingdom)
Web Express, Inc. (United States)
WebTrends (United States)
World-Net (France)
Xin Net Corp. (China)
YesNIC (Republic of Korea)

Companies that have qualified for accreditation as post-testbed registrars, but are not yet finally accredited:

1stDomain.Net, a division of G+D International LLC (United States)
9NetAvenue (United States)
ABC Telemedia AG (Germany)
Alldomains.com (United States)
AT&T (United States)
Deutsche Telekom AG (Germany)
Go Daddy Software (United States)
Interdomain (Spain)
NetNames (United Kingdom)
NETPLEX LLC (United States)
Nobel Networks (United States)
pair Networks, Inc, d/b/a pairNIC (United States, United Kingdom, and Germany)
Parava Networks, Inc. (United States)
RCN (United States)
REACTO.com Ltd. (United Kingdom)
Telepartner AS (Denmark)
Verio (United States)
Virtualis Systems, Inc. (United States)

ANEXO 4 : COMUNICADO DEL GAC EN EL CAIRO

Governmental Advisory Committee - Communique

WEDNESDAY, 8 MARCH 2000 - The Governmental Advisory Committee of the Internet Corporation for Assigned Names and Numbers held its fifth meeting yesterday and today in Cairo. The attending Committee members, representing 29 national governments, distinct economies as recognised in international fora, and multinational governmental and treaty organisations, reflecting representation from all of ICANN's geographic regions, issued the following statement:

The Governmental Advisory Committee (GAC) has had fruitful discussions around substantive issues relating to the usage of the Internet across the worldwide community, ICANN activities, and the administration of the country code top level domains:

A. With regard to the addition of new generic top level domains (gTLDs):

Considering the possibility of expanding the domain name space, the addition of new gTLDs should be done thoughtfully and through a consensus based process. New gTLDs for specific uses, as well as for more generic, or 'open' registration, should be fully considered.

Recognising ICANN's responsibilities to achieve consensus in the creation of any new gTLDs, ICANN should avoid, in the creation of new gTLDs the alpha-3 codes of ISO 3166-1; well known and famous country, territory or regional language or people descriptions; or ISO 639 codes for representation of languages, unless in agreement with the relevant governments or public authorities.

B. With regard to the delegation and administration of country code top level domains (ccTLDs):

The GAC Document "Principles for the Delegation and Administration of Country Code Top Level Domains" represents the views of the national governments, distinct economies and multinational governmental and treaty organisations that comprise the GAC. The text of the document is the result of careful consideration by the GAC, and stands as a whole.

The GAC engaged in a discussion with the ccTLD Constituency of the DNSO on issues concerning administration and delegation of ccTLDs. The GAC notes the invitation by the representatives of the ccTLD Constituency to participate in further constructive discussions regarding the framework for administration and delegation of ccTLDs, with a view towards providing advice to the ICANN Board by its next meeting in Yokohama.

The GAC welcomes this goal and believes that further discussions will be most productive after the ccTLD Constituency has agreed upon a unified text. The GAC also welcomes the efforts of the ccTLD community to develop best practices.

C. With regard to ICANN's At Large Membership and process:

Given the significance of the At-Large Membership and elections to the ICANN process, the manner in which the process is conducted is of significant interest to the GAC. The GAC considers that priority on the establishment of an At-Large Membership should be in establishing a fair and effective process for elections. As ICANN moves forward, the GAC urges ICANN to consider the extension of the September 30 deadline, if necessary, in order to meet this important objective. The need to reflect language diversity, as an essential element for the fairness of elections, was also emphasised.

D. With regard to future workplans:

The GAC has identified areas of future consideration, including

- issues in relation to ICANN's present documentation for the identification of current ccTLD administrators
- ICANN funding and budget
- further discussion on intellectual and other property issues, including warehousing and speculation in domain names
- International character sets within the DNS
- further discussion on ISO 3166
- further discussion on new gTLDs

The GAC thanks the Egyptian government, the Cairo Host Committee, the Internet Society of Egypt and the sponsors for hosting its meeting.

The next face-to-face meeting of the GAC will be held in Yokohama to coincide with ICANN's next round of meetings.

Los Delitos Informáticos en el Ciberespacio en la Legislación Peruana

Dr. Julio Núñez Ponce (Perú)
Catedrático de Derecho Informático en la Universidad de Lima. Magíster en Derecho Empresarial.
Doctorando en Derecho. Autor de los libros : Derecho Informatico y Software:
Licencia de Uso, Derecho y Empresa.

I. INTRODUCCION.

Las Tecnologías de la información y las redes de computadoras plantean una serie de problemas jurídicos que el derecho debe solucionar eficazmente. Entre éstos tenemos los delitos informáticos, que definimos como : *actos antijurídicos, culpables debidamente tipificados* que para su comisión utilizan elementos informáticos (hardware, software) o atentan los derechos del titular de un elemento informático. Recientemente, el ingreso de un ciberpirata o hacker a la página web de la Oficina Nacional de Procesos Electorales (ONPE) ha puesto sobre el tapete *el tema de los delitos informáticos.*

Para que efectivamente las sanciones penales puedan aplicarse adecuadamente en el ámbito informático es *necesario que se solucionen temas relacionados* con la jurisdicción y competencia en Internet, los criterios para determinar la aplicación de la ley penal en el ciberespacio, la prueba informática y la debida tipificación de las conductas criminales que se originan en las redes de computadoras.

El objetivo de la presente ponencia, es analizar desde el punto de vista de la legislación peruana, los avances e iniciativas presentadas en torno al tema de los delitos informáticos en el ciberespacio. Para lo cual se hace el seguimiento de avances en esta materia en nuestro país.

II.- LOS DELITOS INFORMATICOS EN LA LEGISLACION PERUANA Y EL PROYECTO DE LEY PRESENTADO SOBRE LA MATERIA.

En el Perú, en el Código Penal encontramos figuras delictivas que se encuadran dentro de la definición que hemos señalado, que son las siguientes :

a) Delito de Violación a la Intimidad.

En nuestro Código Penal está tipificado en el artículo 154 el Delito de violación a la intimidad, y establece que : "el que viola la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios será reprimido con pena privativa de libertad no mayor de dos años. La pena será no menor de uno ni mayor de tres y de treinta a ciento veinte días cuando el agente revela la intimidad conocida de la manea antes prevista".

El artículo 157 del Código Penal precisa que "el que indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida intima de una o más personas será reprimido con pena privativa de libertad no menor de un año ni mayor de cuatro años. Si el agente es funcionario o servidor público y comete delito en ejercicio del cargo, la pena será no menor de tres. años ni mayo de seis e inhabilitación". Las base de datos computarizadas consideramos que están dentro del precepto de "cualquier archivo que tenga datos", en consecuencia está tipificado el delito de violación a la intimidad utilizando la informática y la telemática a través del archivo , sistematización y transmisión de archivos que contengan datos privados que sean divulgados sin consentimiento.

b) Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas.

El artículo 185 del Código Penal establece que aquella persona que "... para obtener provecho, se apodera ilegítimamente de un bien total o parcialmente ajeno, sustrayéndolo del lugar donde se encuentra, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años. Se equipara a bien mueble la energía eléctrica, el gas, el agua y cualquier otro elemento que tenga valor económico, así como el espectro electromagnético".

El artículo 186 del Código Penal , segundo párrafo numeral 3 - modificado por la ley 26319- dispone además "la pena será no menor de cuatro años ni mayor de ocho si el hurto es cometido mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o la violación del empleo de claves secretas". El delito de hurto agravado por transferencia electrónica de fondos tiene directa importancia en la actividad informática.

El sistema de transferencia de fondos , en su conjunto, se refiere a la totalidad de las instituciones y prácticas bancarias que permiten y facilitan las transferencias interbancarias de fondos. El desarrollo de medios eficientes de transmisión de computadora a computadora de las órdenes de transferencia de fondos ha fortalecido el sistema. Los niveles de calidad y seguridad de las transferencias interbancarias de fondos se han ido acrecentando conforme el avance de la tecnología, no obstante la vulnerabilidad a un acceso indebido es una "posibilidad latente" por tanto además de los sistemas de seguidad de hardware , software y comunicaciones ha sido necesario que la norma penal tenga tipificada esta conducta criminal.

Uno de los medios de transferencia electrónica de fondos se refiere a colocar sumas de dinero de una cuenta a otra, ya sea dentro de la misma entidad financiera o una cuenta en otra entidad de otro tipo, ya sea pública o privada. Con la frase "telemática en general" se incluye todas aquellas transferencias u operaciones cunatificables en dinero que pueden realizarse en la red informática ya sea con el uso de Internet , por ejemplo en el Comercio Electrónico o por otro medio. Cuando se refiere a "empleo de claves secretas" se está incluyendo la vulneración de password, de niveles de seguridad, de códigos o claves secretas.

c) Delito de Falsificación de Documentos Informáticos.

El Decreto Legislativo 681 modificado por la Ley 26612, es la norma que regula el valor probatorio del documento informático, incluyendo en los conceptos de microforma y microduplicado tanto al microfilm como al documento informático. El artículo 19 de esta norma establece que : "la falsificación y adulteración de microformas, microduplicados y microcopias sea durante el proceso de grabación o en cualquier otro momento, se reprime como delito contra la fe pública, conforme las normas pertinentes del Código Penal".

Las microformas que cumplidos los requisitos técnicos (equipos y software certificados que garantizan inalterabilidad, fijeza , durabilidad, fidelidad e integridad de documentos micrograbados) y formales (que procesos de micrograbación sean autenticados por un depositario de la fe pública, por ejemplo el fedatario juramentado en informática) sustituyen a los documentos originales para todos los efectos legales.

En el Código Penal Peruano (C.P.), entre los delitos contra la fe pública, que son aplicables a la falsificación y adulteración de microformas digitales tenemos los siguientes :

i) Falsificación de documentos. "El que hace, en todo o en parte, un documento falso o adultera uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho con el propósito de utilizar el documento, será reprimido, si de su uso puede resultar algún perjuicio, con pena privativa de libertad no menor de dos ni mayor de diez años..." (Artículo 427 del C.P.). Trátandose de microformas digitales su falsficación y/o adulteración son sancionados con la misma pena.

ii) Falsedad ideológica "El que inserta o hace insertar , en instrumento público , declaraciones falsas concernientes a hechos que deben probarse con el documento, con el propósito de emplearlo como si la declaración fuera conforme a la verdad, será reprimido si de uso puede re-

sultar algún perjuicio , con pena privativa de libertad no menor de tres ni mayor de seis años.." (Artículo 428 del C.P.). Hay que tener en cuenta que la microforma digital de un documento público tiene su mismo valor, por tanto puede darse el caso de falsedad ideológica de instrumentos públicos contenidos en microformas digitales.

iii) Omisión de declaración que debe constar en el documento. "El que omite en un documento público o privado declaraciones que deberían constar o expide duplicados con igual omisión al tiempo de ejercer una función y con el fin de dar origen a un hecho u obligación , será reprimido con pena privativa de libertad no menor de uno ni mayor de seis" (Artículo 429 del C.P.). Para que tenga valor probatorio y efecto legal una microforma digital tiene que cumplir requisitos formales y técnicos. El requisito formal consiste en que debe ser autenticado por depositario de la fe pública (fedatario juramentado o notario) el proceso técnico de micrograbación y que las copias de esos documentos deben ser certificados, por lo cual una omisión de las declaraciones que por ley deben incluirse podría configurar esta figura delictiva.

d) Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos.

Puesto que en el patrimonio de la persona están incluidos tanto bienes materiales (hardware) como inmateriales (software, información, base de datos,etc) esta figura delictiva puede aplicarse al campo informático según interpretación del artículo 198º inciso 8 del Código Penal, establece que : "será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años el que, en su condición de fundador, miembro del directorio o del consejo de administración o del consejo de vigilancia, gerente, administador o liquidador de una persona jurídica, ealiza, en perjuicio de ella o de terceros, cualquiera de los actos siguientes : Usar en provecho propio o de otro, el patrimonio de la persona (inciso 8). Esta figura podría aplicarse, en este orden de ideas, tanto al uso indebido de software, información, datos informáticos, hadware u otros bienes que se incluyan en el patrimonio de la persona jurídica.

e) Delito contra los derechos de autor de software.

Con respecto a los delitos contra los derechos de autor de software, debe tenerse en cuenta que "...sobre la naturaleza jurídica y la tutela que apunta el derecho de autor sobre el software hay acuerdo general. Y no puede ser de otro modo, debido a la trascendencia que tiene, dado que la transgresión de índole penal ala actividad intelectual constituye no sólo una agresión a la propiedad del autor y afecta los intereses de la cultura, sino que conforma también un ataque al derecho moral sobre la paternidad de la obra".[1]

Con la dación del Decreto Legislativo 822, se modificó el Código Penal y se han aumentado las penas, con respecto a la legislación peruana anterior, así tenemos:

i) Que el artículo 217º del Código Penal Peruano establece que "será reprimido con pena privativa de libertad no menor de dos ni mayor de seis años y con treinta a noventa días-multa, el que con respecto a una obra,...o una grabación audiovisual o una imagen fotográfica expresada en cualquier forma, realiza cualquiera de los siguientes actos, sin la autorización previa y escrita de autor o titular de los derechos.

a) la modifique total o parcialmente.

b) La reproduzca total o parcialmente, por cualquier medio o procedimiento.

c) La distribuya mediante venta, alquiler o préstamo público.

[1] LEDESMA, Julio C.:"Derecho Penal Intelectual" Ed. Universidad. Buenos Aires, Argentina. 1992. págs. 194,195.

d) La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.
e) La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

Aquí se están garantizando bajo la protección los derechos patrimoniales; en los contratos de licencia de uso de software se contemplan el respeto de estos derechos y también en la Ley de Derecho de Autor que anteriormente hemos tratado. La autorización previa y escrita del titular, generalmente en la activad empresarial se instrumenta en una licencia de uso de software.

ii) Que el Artículo 218º del Código Penal Peruano dispone que "la pena será privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento veinte días-multa cuando:

a) Se de a conocer a cualquier persona una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular.

b) La reproducción, distribución o comunicación pública se realiza con fines de comercialización, o alterando o suprimiendo, el nombre o seudónimo del autor, productor o titular de los derechos.

c) Conociendo el origen ilícito de la copia o reproducción, la distribuya al público, por cualquier medio, la almacene, oculte, introduzca al país o la saca de éste.

d) Se...ponga de cualquier otra manera en circulación dispositivos, sistemas, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas; o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no estén autorizados para ello.

e) Se inscriba en el Registro del Derecho de Autor la obra,... como si fuera propia, o como de persona distinta del verdadero titular de los derechos.

Los supuesto tratados en este artículo se refieren tanto a derecho morales como patrimoniales, que por su gravedad (atentar contra el derecho de paternidad, comercializar o distribuir copias ilegales, registrar en forma indebida el software) se amplía la pena hasta ocho años. En la anterior legislación la pena mayor por este tipo de delitos era de cuatro años, actualmente se ha aumentado a ochos años. Estos tipos penales, parten del supuesto que no hay consentimiento o autorización del titular de los derechos para ello; de existir una licencia de uso y cumplirse con sus términos y condiciones, no se tipificaría este delito.

iii) Que el Artículo 219º del Código Penal Peruano, establece que :"será reprimido con pena privativa de libertad no menor de dos ni mayor de ocho años y sesenta a ciento ochenta días-multa, el que con respecto a una obra, la difunda como propia, en todo o en parte, copiándola o reproduciéndola textualmente, o tratando de disimular la copia mediante ciertas alteraciones, atribuyéndose o atribuyendo a otro, la autoría o titularidad ajena".

La apropiación de autoría ajena, de reputarse una obra que no es de uno como propia, también se aplica la software, más aún con las opciones tecnológicas para su copia, que incluyen equipos de cómputo, cada vez más sofisticados y el uso de herramientas en Internet.

iv) Que el Artículo 220º del Código Penal Peruano, dispone que: " será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y noventa a trescientos sesentaicinco días-multa:

a) Quien se atribuya falsamente la calidad de titular originario o derivado, de cualquiera de los derechos protegidos en la legislación del derecho de autor y derechos conexos y, con esa indebida atribución, obtenga que la autoridad competente suspenda el acto de comunicación, reproducción o distribución de la obra, interpretación, producción, emisión o de cualquier otro de los bienes intelectuales protegidos.

...

e) Si el agente que comete cualquiera de los delitos previstos... posee la calidad de funcionario o servidor público.

Una de las preocupaciones de los creadores de software, al registrar su obra en el Registro Nacional de Derecho de Autor de INDECOPI, es que se tiene que entregar, entre otros requisitos, el programa fuente, se cuestionan que sucede si lo copian sin su consentimiento. Dado que el depósito es intangible, los funcionarios que cometieran estos delitos estarían dentro de este tipo penal y podrían ser pasibles de pena privativa de libertad hasta ocho años.

En el Congreso de la República del Perú se ha presentado el Proyecto de Ley 5071/99 que propone incorporar dentro del Título V de los delitos contra el patrimonio el capítulo XI que contendría los siguientes artículos :

Artículo 208A.- "El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadora o a cualquier parte de la misma, con el propósito de diseñar, ejecutar, copiar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de libertad no mayor de dos años, o con prestación de servicios comunitarios de de cincuentidos a ciento cuatro jornadas ".

Artículo 208B.- "El que indebidamente interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de libertad no mayor de dos años".

Con respecto, a estos artículos del proyecto de ley, señalamos los siguientes comentarios :

i) "Somos de la opinión que debiera evaluarse la conveniencia de aumentar las penas para coadyuvar en su eficacia y que guarde similitud con las penas de los delitos informáticos ya tipificado en nuestro ordenamiento jurídico, por lo que debiera aumentarse hasta ocho años" [2]

ii) "Este tipo de criminalidad es de reciente aparición. Comenzó a manifestarse con los llamados computer hackers, personas especialmente hábiles en el manejo de la informática, quienes hicieron sonar la alarma de la necesidad de reforzar la seguridad en estos sistemas. En los pasados trece meses se han registrado catorce mil ochocientos veintiséis ataques de los piratas del ciberespacio en todo el mundo. En el Perú se han registrado veintisiete de estas transgresiones"[3]

iii) En diversas páginas web peruanas se ha detectado acceso indebido y presencias de hackers, que por lo general son informáticos que se introducen para alterar información. Se ha podido hacer un seguimiento del posible origen de estos hackers, señalándose los países de Francia, Brasil, Israel, Irak, Alemania, España, Canadá y Estados Unidos como los lugares desde donde se han originado los mensajes y las conexiones para el acceso indebido de las páginas web peruanas.

iv) Frente a estos hechos se afirma que se justifica los artículos señalados, en este capítulo del proyecto de ley sobre delitos informáticos.

---

[2] *Opinión sostenida por el Dr. Julio Núñez Ponce, Catedrático de Derecho Informático en la Universidad de Lima.*

[3] Criminalidad Telemática. Diario Oficial "El Peruano" . Lima, Viernes 18 de Febrero de 2000. Página 10.

III.- ANALISIS DE LOS ARTICULOS 208A Y 208B PROPUESTOS EN EL PROYECTO DE LEY PERUANO 5071/99

El Proyecto de Ley 5071/99 que actualmente está en la Comisión de Reforma de Códigos del Congreso de la República del Perú, propone en el Artículo 208A lo siguiente :

... "El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadora o a cualquier parte de la misma"... El acceso indebido o no autorizado a base de datos computarizadas, a sistemas interconectados en red incluida Internet o a cualquier parte de la memoria del computador, estaría en el supuesto de esta figura delictiva propuesta. Quien accese indebidamente, incluidos los hackers estarían comprendidos en este supuesto. Los hackers son esa legión de jóvenes fanáticos de la informática con un computador personal, con un módem y una gran imaginación que son capaces de acceder a través de una red pública de transmisión de datos al sistema informático de una organización, entidad o empresa.

..." con el propósito de diseñar, ejecutar, copiar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido"... el propósito doloso que tipificaría esta forma delictiva estaría en que este acceso indebido originaría :

- el diseño de un esquema o artificio que se crea en el momento del acceso indebido.
- la ejecución o copia de un software ya creado anteriormente con una finalidad ilegal.
- la alteración o modificación de un software existente variándose su finalidad de lícita a ilícita.

La finalidad ilegal se precisa que consistiría :

i) En la defraudación. El engaño, ardid y astucia utilizados electrónicamente como finalidad de acceso indebido.

ii) Obtención de dinero. La sustracción de dinero electrónico ; este supuesto ya está legislado en el artículo 186 inciso 3 del Código Penal Peruano al referirse a transferencia electrónica de fondos, por lo cual el proyecto debiera revisarese en ese aspecto.

iii) Bienes o información. Se incluye los bienes muebles inmateriales como son el software, el shareware, las base de datos, la información.

... "con pena privativa de libertad no mayor de dos años, o con prestación de servicios comunitarios de de cincuentidos a ciento cuatro jornadas "... Las pena propuesta no guarda relación con la pena de hasta ocho años de pena privativa de libertad ya tipificada en el Código Penal Peruano para el delito de hurto agravado por transferencia electrónica de fondos, uso de la telemática y vulneración de claves secretas, conforme el artículo 186 inciso 3, por lo cual la pena propuesta debiera ser mayor.

Asimismo, el Proyecto de Ley 5071/99 que actualmente está en la Comisión de Reforma de Códigos del Congreso de la República del Perú, propone en el Artículo 208B lo siguiente :

..."El que indebidamente interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma..." En esta figura delictiva se está incluyendo el sabotaje informático y los daños producidos por los virus informáticos, con lo cual se cubiría un vacío legal que es necesario tener presente en la armonización legislativa que debe realizarse sobre esta materia.

..."en la base, sistema o red"... estos daños, alteraciones, sabotajes informáticos que destruye el soporte, el software o datos deben estar contenidos en la base de datos, sistema o red que utilice la entidad, organización o empresa, en estos supuestos se incluye internet, intranet y extranet.

..."será reprimido con pena privativa de libertad no mayor de dos años" La pena propuesta también debiera ser aumentada hasta ocho años, para que guarde similitud con los otros delitos informáticos tipificados en el ordenamiento jurídico peruano.

IV.- TEMAS RELACIONADOS PARA UNA ADECUADA SANCION DE LOS DELITOS INFORMATICOS EN EL CIBERESPACIO.

En diversos países y foros internacionales se ha expresado preocupación por la incidencia rápidamente creciente de los delitos vinculados con la tecnología moderna y cometidos con su ayuda. "Esas nuevas formas de delincuencia requieren el aprovechamiento compartido de conocimientos especializados y experiencias a nivel nacional e internacional, así como la adaptación de la legislación existente o la adopción de otra nueva que tuviera en cuenta las características regionales. ..Debido a que el uso de las computadoras y redes informáticas ha facilitado nuevas formas de delincuencia, existe la necesidad de elaborar un nuevo instrumento jurídico internacional que previera la investigación, el enjuiciamiento y la sentencia a nivel transfronterizo por delitos relacionados con el uso indebido de las redes informáticas"[4]. Esta necesidad a nivel internacional requiere que los países a nivel regional (en este caso, a nivel de las Américas) tengan elementos comunes y tomen decisiones conjuntas sobre esta materia y adopten posiciones sobre los temas relacionados siguientes :

a) La jurisdicción y competencia en Internet.- Es necesario determinar criterios para determinar que jurisdicción se aplica y quien es el juez competente en los delitos cometidos en las redes informáticas interconectadas como Internet.

b) Los criterios para determinar la aplicación de la ley penal en el ciberespacio.- Que implica la solución de una serie de supuestos en la transferencia electrónica de fondos, en la transferencia electrónica de datos informatizados, en el acceso indebido de datos, en la proliferación de hackers y la vulneración de información que infirngen bienes jurídicos protegidos de varios países simultáneamente.

c) La prueba informática.- Es un aspecto fundamental a tenerse en cuenta, la aceptación del valor probatorio del documento informático para el proceso penal por parte de los jueces.

d) La debida y similar tipificación de las conductas criminales que se originan en las redes de computadoras.- Que requiere una armonización legislativa y un efectivo intercambio de información entre los diversos países.

En las conclusiones y recomendaciones de la Segunda Reunión de Ministros de Justicia, en Marzo de 1999 en Lima, Perú, con respecto al delito cibernético se recomendó la constitución de un grupo de expertos gubernamentales en el marco de la OEA que hiciera un diagnóstico de la actividad delictiva, legislación, políticas y prácticas nacionales e indentificar las entidades con experiencia en la materia y los mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético. Para estos efectos, el grupo de expertos presenta un informe en la III Reunión de Ministros de Justicia.

Consideramos, que se está avanzando en el camino correcto, las reflexiones planteadas e información proporcionada tiene por fin coadyuvar en estos objetivos comunes.

[4] Naciones Unidas. Informe de la Reunión Preparatoria Regional de Asia Occidental sobre prevención del Delito y tratamiento del Delincuente. Beirut del 11 al 13 de Noviembre de 1998. A/Conf.187/RPM.2/1. Numeral 44.

BIBLIOGRAFIA

- CONSENTINO, Guillermo et Al :"Tras los pasos de la Seguridad Perdida :Delitos Informáticos". En Revista Iberoamericana de Derecho Informático Nº 25. Mérida, España. UNED. 1998.

- DAVARA, Miguel Angel : "Derecho Informático". Editorial Aranzandi España, 1993.

- TIEDEMAN, Klaus : "Criminalidad mediante Computadoras". En Poder Económico y Delito. Editorial Ariel S.A. Barcelona 1985.

- TELLEZ VALDES, Julio : "Derecho Informático". Segunda Edición. Editorial McGraw-Hill. México 1997.

- NUÑEZ PONCE, Julio César : "Software : Licencia de Uso, Derecho y Empresa". Fondo de desarrollo Editorial de la Universidad de Lima. Lima, 1998.

- LEDESMA, Julio C.:"Derecho Penal Intelectual" Ed. Universidad. Buenos Aires, Argentina. 1992. págs. 194,195.

Tema 2

NUEVOS DESAFIOS AL DERECHO INFORMATICO AL NUEVO MILENIO

La Nueva Ley Española de Protección de Datos de Carácter Personal

Valentín Carrascosa López (España)
Doctor en Derecho. *Presidente de FIADI y Director Centro Regional de Extremadura de UNED*

I. LA NUEVA LEY ESPAÑOLA DE PROTECCION DE DATOS DE CARACTER PERSONAL (L.O.P.D.)

1. INTRODUCCION

El pasado día 14 de enero de 2.000, entró en vigor la nueva Ley Orgánica de Protección de Datos de Carácter Personal[1], que deroga la LORTAD[2] por la necesidad de adaptar dicha norma a la Directiva[3] General de Protección de Datos de la Unión Europea.

La LOPD otorga más facilidades al tráfico mercantil, a costa de suavizar la defensa del derecho a la intimidad, garantizado por la Constitución. Además de mantener los preceptos de la Ley de 1992 impugnados ante el Tribunal Constitucional -entre otros, por el PP- por posible vulneración de derechos fundamentales desde los ficheros públicos.

La nueva Ley autoriza el uso y tratamiento privado de los datos del censo electoral y permite a las aseguradoras establecer ficheros comunes que entrecrucen datos personales.

La Directiva configura derechos subjetivos que integrarían el haz de derechos que forman el derecho fundamental de la autodeterminación informativa, que junto con los derechos de información (art. 5), consentimiento y oposición (art. 6),consulta (art. 14), acceso (art. 15), rectificación y cancelación (art. 16) y otros configurados por la nueva Ley Orgánica de Protección de Datos,sientan el soporte legal para la protección de datos, pero, según Aspas[4] las nuevas redes digitales avanzadas de telecomunicación, especialmente la red digital de servicios integrados (RDSI) y las redes móviles digitales crean necesidades especificas de protección de los derechos fundamentales, especialmente de la intimidad, a través de protección de datos.

Determinadas características nuevas de los servicios, especialmentente en el ámbito de los servicios telefónicos, por ejemplo: la identificación de la línea de llamada y linea conectada, el servicio de transferencia o desvío automático de llamadas y los teléfonos móviles, así como los dispositivos de búsqueda de llamadas malintencionadas o los dispositivos automáticos de llamada; la elaboración de facturas telefónicas en las que se detallan los números que han sido objeto de llamadas; la difusión de las guías de abonados, en soporte papel o electrónicas, facilitan información sobre la vida privada que pueden dar a abusos e ingerencias no deseadas y esta preocupación por la protección de los derechos fundamentales, especialmente de la intimidad, ha llevado a la Unión Europea a adoptar la Directiva 97/66/CE, del Parlamento y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, complementaria de la Directiva 95/46/CE.

Si la sociedad, para su desarrollo,tal y como está concebida hoy día demanda datos y más datos, pues, segun Alvarez Cienfuegos,[5] la información, de la índole que sea, se ha convertido en bien jurídico de extraordinario valor, hasta el punto de que son muchos los que hoy califican a la información como el auténtico poder de las sociedades avanzadas, pero la libertad de la información, bien jurídico cada día más demandado como objeto de con-

---

1 La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante "LOPD" fue publicada en el BOE de 14 diciembre 1999.

2 La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, en adelante "LORTAD".

3 La Directiva-95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante "Directiva".- Diario Oficial de la Comunidad Europea núm. L 281, de 23 de noviembre de 1995.

4 Aspas Aspas, José Manuel, "Las guías de servicios de telecomunicaciones y la protección de datos", La Ley 4966 de 10 de enero de 2000.

5 Alvarez-Cienfuegos Suárez, José María, La Defensa de la Intimidad de los Ciudadanos y la Tecnología Informática, Aranzadi, Año 1999, Pág. 13.

sumo de las sociedades avanzadas, no puede concebirse sin el contrapunto de salvaguarda o defensa de datos personales que afecten a la intimidad personal y familiar y para ello nos encontramos, entre otros preceptos, con el art. 18 de la Constitución y ahora con la LOPD.

Para que los intereses protegidos por el art. l8 de la Constitución sean efectivos, es decir realmente protegidos, era necesario una serie de normas como La LORTAD, y otras anteriores a ella, pero tambien ha sido necesario la aprobacion de una serie de normas, completarias de la anterior y que, aunque sea someramente, conviene citar: el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos; el Real Decreto 1332/94, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica, fundamentalmente el proceso de incripción de ficheros, la regulación del efectivo ejercicio de los derechos de acceso, rectificación y cancelación y los Procedimientos Sancionador y de Tutela de Derechos de la Agencia de Protección de Datos; el Real Decreto 156/1996, ded 2 de febrero, por el que se modifica el Estatuto de la Agencia de Protección de Datos, para designarla como representante español a los efectos previstos en el art. 29 de la Directiva 95/46/CE; las Ordenes Ministeriales de 2 de febrero de 1995 y 31 de junio de 1998 del Ministerio de Justicia, por las que se aprueba y ampliá la relación de paises con proteccion de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos y el Real Decreto 994/1999, de 11 de junio, que seguiran en vigor, por mandato de la disposicion transitoria tercera de la LOPD hasta tanto no se lleven a efecto la previsiones de la disposición final primera de la LOPD que faculta al Gobierno a aprobar o modificar las disposiciones reglamentarias necesarias para la aplicacion y desarrollo de la presente Ley.

Es obvio, como dicen Del Peso y Ramos[6] que la Directiva Europea 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos no ha podido ser antecedente de la LORTAD, pues su publicación es posterior a ésta.

Sin embargo sí se puede considerar que lo es la Propuesta de Directiva que la Comisión Europea presento al Consejo el 18 de julio de 1990, que aun que sufrió una serie de modificaciones ya adelantaba el propósito de la Unión de aproximar las diferencias existentes entre las legislaciones de los países miembros al objeto de elimitar los obstáculos a la circulación de datos personal y conseguir un nivel de protección de los derechos y libertades de la persona, que llevo a que la LORTAD naciese ya incorporando los principales principios, que estableceria despues la Directiva.

Tal situación, creo, es la que llevo al actual Director de la Agencia de Protección de Datos,[7] a manifestar que a su modo de ver, no había ninguna necesidad de la actual ley. De hecho, lo que el gobierno remitio a las Cortes fue un proyecto de ley de reforma parcial. Por motivos que desconozco, lo que en el Parlamento se decidió fue hacer una nueva ley, sin ser necesario y sin que la nueva ley aportase grandes ventajas sobre la ya existente, pero lo cierto es que la nueva Ley de Protección de Datos de Carácter Personal fue aprobada con muchas modificaciones - a través de más de 100 enmiendas introducidas en el trámite parlamentario en el Senado - sobre el texto original, por lo que seguiremos el estudio apoyandonos en la LOPD pero teniendo en cuenta la LORTAD pues si bien se ha cambiado el fin último, permanece vigente gran parte de su artículado.

Tras esta introducción nuestro objetivo es reflexionar sobre cuál sea la razón de ser y la finalidad de la LOPD, pero fundamentalmente cómo esta norma puede proteger la vida privada, todo ello con riesgo de equivocarnos al ser la LOPD una ley, recientísima, sobre la que no hay doctrina a la que acudir porque no la puede haber, pues no ha habido tiempo para crearla.

2. EL OBJETO Y LA FINALIDAD

La aplicación de la LOPD no va estar exenta de dificultades, toda vez que carece de Exposición de Motivos y no existe una jurisprudencia interpretativa consolidable.

---

6 Del Peso Navarro, Emilio y Ramos González, M. A., LORTAD-REGLAMENTO DE SEGURIDAD, Diaz de Santos, Año 1999, Pág. 11.

7 Fernández López, Juan Manuel, "en entrevista a Daniel Conejero", AUSBANC -Asociación de Usuarios de Servicios Bancarios, Nº 115, Enero 2000, Pág. 29.

La LORTAD, por el contraria, tenía una amplia exposición de motivo y así vemos como en el apartado primero de la exposicion de motivos de la LORTAD concluía señalando que:

" Se hace preciso,pues, delimitar una nueva frontera de la intimidad y del honor, una frontera que, sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esta nueva frontera es el objeto de la previsión contenida en el art. 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley ". Y reiteraba al inicio de su apartado segundo "... que su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, la Ley se nuclea en torno a los que convencionalmente se denominan "ficheros de datos ": Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad....."

Al objeto se refería el artículo lº de la LORTAD al señalar:

"La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de caracter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos".

Coincidimos con el Profesor Vilariño[8] cuando dice en relación con la razón de ser de la Ley, el artículo 1º. al transcribir el texto del artículo 18.4 de la Constitución, confunde el mandato constitucional con la verdadera finalidad de las leyes sobre tratamiento automatizado de datos personales, que no es la protección de datos personales, sino la protección de las personas en relación con el tratamiento automatizado de esos datos, como correctamente denomina el Convenio del Consejo de Europa.

De ahí que no sea el honor o la intimidad lo que debe proteger esta Ley, sino el correcto uso y tratamiento de todos los datos de carácter personal, de los que sólo una parte, y pequeña, se refierán a la intimidad.

En definitiva el bien a proteger comprende y supera el de la estricta intimidad, dando pie a la configuración de un nuevo derecho fundamental: el derecho a la AUTODETERMINACION INFORMATIVA[9], pues no se trata de prohibir el uso de la informática, pero si de encaminarlo dentro de unos cauces idóneos para evitar sus peligros, ya que estamos ante la exigencia de ampliar la protección de ciertos derechos en el ámbito en que opera la informática.

Al comparar el artículo 1º de la LORTAD, con el art.1º del Convenio de Estrasburgo y con el art. 1º de la LOPD-,preceptos, todos ellos, referidos al objeto y fin, vemos que estos dos ultimos puntulizan que el fin del mismo no es "limitar" sino el de "garantizar" a cualquier persona física, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal.

En la exposición de motivos queda claro que la finalidad de la LORTAD es hacer frente a los riesgos que para los derechos de la personalidad puedan suponer el acopio y tratamiento de los datos por medios informáticos. Como dice Santamaría Ibeas[10] se trata de asegurar que las garantías de los derechos fundamentales en general y del derecho a la intimidad en concreto no se vean modificados por la aparicion de nuevas técnicas de comunicación, de modo que la estructura tradicional de los derechos fundamentales no sea alterada ni lo que es más importante, reducida respecto de lo que ha sido su normal desarrollo desde el siglo XVIII.

---

[8] Vilariño Pinto, Eduardo. "La Ley de Regulación del Tratamiento Automatizado de Datos de Carácter Personal ante el Derecho Internacional", Barcelona, Generalidad de Cataluña, Año 1993.

[9] Tema suficientemente tratado por Lucas Murillo de la Cueva en su monografía "El Derecho a la autodeterminación informativa" que se publicó en 1990 y continuado con su obra "Informática y protección de Datos Personales" publicada por el Centro de Estudios Constitucionales en 1993.

[10] Santamaría Ibeas, José Javier, "La LORTAD: breve análisis de sus antecedentes", Mérida, UNED MERIDA, Actas del III Congreso Iberoamericano de Informática y Derecho, Vol. Nº 4-5, Año 1992.

Las anteriores reflexiones sobre el objeto y finalidad efectuadas en ponencia dictada[11] en los cursos de verano de la Universidad Complutense de Madrid, son validos ya que la nueva ley lo que hace, en su artículo 1º, es apoyar dicha tesis estableciendo como objeto el garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Podemos, no obstante, decir que el objetivo de la LOPD es más ambicioso pero menos concreto que la LORTAD,pues para esta el objeto era claro:cumplir el mandato constitucional de desarrollar el punto 4 del art. l8 de la Constitucion para limitar el uso de la informatica y otras tecnicas para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derecho.

La LOPD sustituye la palabra limitar de la LORTAD por "garantizar" y "proteger" y al referirse, en el art. 1º, a las libertades públicas y los derechos fundamentales ya no es, su finalidad, un artículo, sino toda la Sección 2ª del Capítulo II del Título I de la Constitución, que comprende del art. 15 al 29 ambos inclusive.

Si vamos al artículo 2 vemos que el ambito de aplicación en la LORTAD se hacia referencia a" los ficheros automatizados de los sectores público y privado" mientras el mismo artículo de la LOPD se refiere a "los datos de caracter personal registrados en soporte físico que los haga susceptible de tratamiento ", diferencias importantes al haber desaparecido el termino automatizados, que nos lleva a considerar que esta ley es aplicable tambien a cualquier otra forma de almacenamiento de datos personales que sea susceptible de tratamiento.

3.- AMBITO DE APLICACION

Aparece definido en el artículo 2 de la LOPD, que hace una acertada declaracion general al considerar que la presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptible de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores públicos o privados.

Del párrafo 1º del artículo 2 se desprende claramente que "la presente Ley será de aplicación a los datos de caracter personal..." es decir se excluye la protección de las personas jurídicas, como ya hacia la LORTAD, y con ello se sigue la opción mayoritaria de no incluir a las personas jurídicas, siguiendo el mismo proceso que la Ley francesa y Directiva y en contraposición a la legislación de Austria, Dinamarca, Luxemburgo y Noruega que incluyen en la protección de dicha normativa tambien a las personas jurídicas.

Siguiendo a Piñoll i Rull y Estadella Yuste[12] cabe manifestar que a pesar de la recomendación a favor de la inclusion en su texto de las personas jurídicas hecha en el informe Bayerl, la Directiva ni nuestra nueva Ley no han recogido tal posibilidad, probablemente ante el temor, subyacente en las directrices de la OCDE, de que tal extensión de la protección de datos a sociedades fuese considerada por Estados Unidos, en especial, como una forma restringida de libre flujo de la información y la libre competencia en los servicios a nivel mundial y, ademas con un interes jurídico protegido mucho menos claro que en el caso de las personas físicas.

Se regirá por la LOPD, conforme al art.2, todo tratamiento de datos de carácter personal: cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento; cuando le sea de aplicación la legislación española en aplicacion de las normas de Derecho Internacional; cuando utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Tras estas declaraciones de principios, que aparenta que la Ley se aplica al tratamiento de datos de persona físicas que se realicen en el ámbito público o privado, afectando a cualquier tipo de ficheros, nos encontramos, en el

---

[11] Carrascosa López, Valentín, LIBERTAD INFORMATICA VERSUS PRIVACIDAD, El Escorial, Año 1995.

[12] Piñoll i Rull, Joan y Estadella Yuste, Olga, "La regulación de la transmisión Internacional de Datos en la L.O.5/1991 de 29 de octubre", Generalitat de Catalunya, Año 1993.

número 2 del artículo 2 menos excepciones que las que contenia la LORTAD e igual regimenes específicos, no siempre justificables, que podrian ser facil excusa para su inaplicacion y sobre todo para poder dejar a la Ley vacia de contenido, al unirse estas excepciones a otras numerosas que aparecen a lo largo de la Ley y que fueron la principal causa de los recursos de inconstitucionalidad planteados contra la LORTAD.

Hay dos tipos de excepciones contenidas en los números 2 y 3 del artículo 2º. de la LOPD.

Según el núm. 2 el régimen de protección de los datos de carácter personal se establece que la presente Ley Orgánica no será de aplicacion: a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; a los ficheros sometidos a la normativa sobre protección de material clasificado; y a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Las excepciones contenidas en el núm 2 son infinitamente inferiores a las que recogía el num. 2 de la LORTAD en la que, entre otros, tambien quedaban exceptuados: el almacenamiento de datos para su publicidad con caracter general; a los de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales; a los ficheros de información jurídica accesible al público; a los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones o comunidades religiosas en cuanto los datos se refiriesen a sus asociaciones o miembros y ex miembros.

En el párrafo tercero, el artículo 2, de la LOPD se hace una nueva exclusión del alcance de la Ley al determinar que se regirán por sus disposiciones específicas:los ficheros regulados por la legislación de régimen electoral; los que sirvan a fines exclusivamente estadísticos al amparo de la Ley de la función estadística pública;los derivados del Registro Civil y del Registro Central de penados y rebeldes; los informes personales de calificacion a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; y los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

En conclusión podemos decir que se ha reducido el numero de excepciones, pero se han añadido algunas nuevas, como la referente a videocamaras por Fuerzas y Cuerpos de Seguridad.

4.- DEFINICIONES

A los efectos de la presente Ley, dice el artículo 3, lo que deberá entenderse por datos de carácter personal, ficheros,tratamiento de datos, responsable del fichero o tratamiento, afectado o interesado y procedimiento de disociación, que ya estaban en la LORTAD, pero a las que añade, algunas que eran totalmente necesarias y por exigencia de la Directiva, cuya transposición se pretende, como nuevas: encargado del tratamiento, consentimiento del interesado, cesión o comunicación de datos y fuentes accesibles al público.

Deciamos[13] que se echaba de menos, en este artículo en la LORTAD, de algunas de las definiciones que ahora recoge la nueva Ley Orgánica de Protección de Datos de Caracter Personal y que hemos recogido en el párrafo precedente pero seguimos pensando que sería bueno la definición de las diferentes categorias de datos de carácter personal, lo que debe entenderse por titularidad pública o titularidad privada, bloqueo de datos,...

5.- PRINCIPIOS DE LA PROTECCION DE DATOS

Al igual que en la LORTAD a los principios de la protección de datos se dedica el título II de la LOPD, que comprende desde el artículo 4 al 12, ambos inclusive, y en los que se regula la calidad de datos, información en la recogida de datos, consentimiento, datos especialmente protegidos, datos relativos a la salud, seguridad de datos, deber de secreto, comunicación de datos -en la LORTAD cesión de datos- y acceso a los datos por cuenta de un tercero.

13 Carrascosa López, Valentín. "LA LORTAD: Una necesidad en el panorama Legislativo Español", UNED MERIDA, Informática y Derecho, Vol. Nº 6-7, Año 1994, Pág. 46.

5.1.- Calidad de los datos

El artículo 4, con el que comienza el titulo II, establece una serie de principios o garantías que podemos sintetizar así: adecuados, pertinentes y no excesivos en relación al ámbito y las finalidades determinadas, explícitas y legitimas para las que se hayan obtenido, no pudiendo usarse para finalidades " incompatibles", en la LORTAD se decia" distintas", con aquellas para las que los datos hubieran sido recogidos; tambien deberan ser exactos y puestos al día de lo contrario serán cancelados y sustituidos de oficio e igualmente deberan ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados; se almacenaran, los datos, de forma que permita el ejercicio del derecho de acceso por parte del afectado; se prohibe la recogida de datos por medios fraudulentos, desleales o ilícitos.

¿Cumplen estos requisitos los datos recogidos a través de las redes "ECHELON", "STORM", "FRANCHELO"... o la propia telefónica?.[14]

5.2 Derecho de informacion en la recogida de datos

El derecho de información en la recogida de datos es tratado, con mayor claridad que en la LORTAD y de forma explicita, en el artículo 5 de la LOPD, al establecer, en todo caso y sin excepción alguna, que los afectados a los que se soliciten datos personales deberán ser previamente imformados de modo expreso, preciso e inequivoco : de la finalidad de la recogida de éstos y de los destinatarios; del carácter obligatorio o facultativo de su respuesta ; de las consecuencias de la obtención de datos o de la negativa a suministrarlos; de los derechos que le asisten respecto al acceso, rectificación, cancelación y,nuevo en la LOPD, oposición; la identidad y dirección del responsable del tratamiento o, en su caso,de su representante en España.

La LOPD introduce, art. 5.4, como novedoso algo que supone una mejor garantía para los ciudadanos, como es, que cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequivoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, excepto cuando expresamente una ley lo prevea o cuando el tratamiento tenga fines históricos, estadisticos o científicos o cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial.

5.3.- Consentimiento del afectado

Una novedad importante es el reforzamiento que la nueva Ley da al consentimiento de los ciudadanos para que sus datos puedan ser tratados. La LORTAD no definía el consentimiento, de lo que sí, en cambio, se ocupa la LOPD en su artículo 3, en el que se exige que el consentimiento sea libre, inequívoco, específico e informado.

Según el artículo 6, salvo que la Ley disponga otra cosa, el tratamiento automatizado de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, olvidandose del resto de requisitos de la definición. Sin embargo, el apartado segundo de dicho artículo contiene varias excepciones ordinarias al disponer que no será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, o cuando se refieran a personas vinculadas por una relación negocial, laboral, administrativa o contractual y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento de las obligaciones, y una excepción de gran amplitud y generalidad, al disponer que no será preciso el consentimiento cuando los datos se recojan " para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias". Con esta excepción, conforme al Profesor Tasende Calvo[15] prácticamente se elimina el consentimiento del afectado como

---

[14] Carrascosa López, Valentín, "Contratación Electrónica, Privacidad e Internet", UNED MERIDA, Informática y Derecho - Revista Iberoamericana de Derecho Informático, Vol. Nº 30-32, Año 1999, Pág. 18 y ss.

[15] Tasende Calvo, Julio: "Notas al Proyecto de la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, Poder Judicial, septiembre 1991

requisito previo al tratamiento automatizado de datos personales por la Administración, a cuyo discrecional exclusivo criterio se encomiento la recogida de tales datos, sin que la ausencia de voluntad del interesado sea suplida por un inmediato control o intervencial judicial o, cuando menos de la Agencia de Protección de Datos.

En todo caso, por esta vía de exclusión del consentimiento se hace inaplicable el artículo 5, sobre la obligación de informar al afectado y, por tanto, se producirá el tratamiento de los datos personales sin conocimiento del interesado.

No cabe consentimiento concedido con carácter general sino que el mismo ha de ser concedido caso por caso.

La exigencia fundamental del consentimiento del afectado para el tratamiento automatizado de datos de carácter personal, sólo podrá ser revocado, conforme al número tercero del artículo 6, cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

Como hemos dicho, el art. 6.1., enuncia la regla capital en materia de protección de datos: el consentimiento y por ello este aparece en varios preceptos de la ley y que en algunos casos ha de ser necesariamente expreso y prestarse por escrito (art. 7.2 y 3), de ahí que los derechos de información, acceso, rectificación y cancelación así como los demás que contamplaba la LORTAD en su título III y ahora el capitulo III de la LOPD, no sean, siguiendo a Lucas Murillo de la Cueva, sino una manifestación específica, una proyección concreta, de este elemento capital, del mismo modo que lo son las facultades que los artículos 11.1 y 3, 21.3, 28.2,29.1, 30.1 reconocen a la persona a la que se refieren los datos.

El legislador, para asegurar una mayor protección, ha acotado claramente el marco en el que ese consentimiento se presta en cada ocasión, poniendo, igualmente los medios necesarios para asegurar que el uso que de ellos se hace concuerdan con los términos en que expresó su voluntad.

Podemos concluir, con el consentimiento del afectado, diciendo que ésta es la piedra angular a partir de la que se construye el sistema de protección de datos personales frente al uso de la informática.

5.4.- Datos especialmente protegidos

Bajo el epígrafe de datos especialmente protegidos encuadra el artículo 7, algunos datos de carácter personal, que se ha convenido en denominar "datos sensibles", expresión nueva en nuestro lenguaje jurídico y a los que la LORTAD quería, y ahor a la LOPD, proteger de una manera especial.

Se incluyen entre ellos,en el número 2, los que se refieren a la ideología, afiliación sindical, religión y creencias. Siguiendo a la Directiva, la LOPD incorpora entre los datos especialmente protegidos a los "sindicales". Si bien no estaban éstos expresamente recogidos en la LORTAD entre los de esta categoría,venían obteniendo esta mayor protección toda vez que, como ha señalado nuestro Tribunal Constitucional, deben aquéllos incluirse entre los que revelan ideologías.

El núm.3, incluye, los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual. El num. 5 del citado artículo incluye tambien a los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, dentro de los datos especialmente protegidos.

La Ley no da la misma protección a todos estos datos y siguiendo a Murillo de la Cueva, distinguiremos, de acuerdo con las previsiones de la Ley, tres categorías :

En la primera figuran los datos sobre la ideología, afiliación sindical, religión y creencias. Las especialidades que revisten los mecanismos ideados para protegerlos consisten en la exigencia de que el consentimiento se exprese por escrito y de manera explícita (art. 7.2). Además será necesario que, cuando se recabe la autorización, se advierta especialmente al interesado de su derecho a no prestar, ya que estos aspectos de la personalidad gozan de amparo constitucional específico, al establecer el artículo 16.2 de la CE que " nadie podrá ser obligado a declarar sobre su ideología religión o creencias".

En la segunda se hallan los datos que afectan al origen racial, la salud y la vida sexual. En este caso, el artículo 7.3 establece, como ya hemos dicho anteriormente, que sólo podrán ser recabados, tratádos y cedidos cuando el afectado otorgue su consentimiento expreso o en los supuestos en que, por razones de interés general, una ley así lo disponga. La excepción que permite prescindir, en materia tan delicada, de la voluntad del afectado está justificada, ya que parece suficiente garantía sustituirla por una habilitación del legislador fundada en razones de interés general, Ley que por otra parte tendrá el carácter de Orgánica, dado el carácter de Ley Orgánica del artículo 7 y por la naturaleza de información que estamos contemplando.

Como hemos indicado, en el núm.5 del artículo 7, nos encontramos con una tercera categoría, la constituida por los datos personales referentes a infracciones penales o administrativas, los cuales solamente podrán figurar en los ficheros automatizados de las Administraciones públicas, siempre que estas sean competentes en la materia y que tengan lugar en los supuestos, expresamente, previstos, en sus normas reguladoras.

El legislador, en su deseo de disuadir en el tratamiento indebido de estos datos, al tipificar, en el art.44, las infracciones, califica de muy graves " recabar y tratar los datos de carácter personal a los que se refiere el apartado 2, del artículo 7, cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del art. 7" (artículo 44.4.c) e igualmente en el artículo 45 al determinar los tipos de sanciones, expresa, en su número 4, que " la cuantía de las sanciones se graduarán atendido a la naturaleza de los derechos personales afectados....."

5.5 Datos relativos a la salud

Las informaciones relativas a la salud son informaciones especialmente sensibles a la que el legislador español ha proporcionado una especial protección en diversas normas[16] que van desde la Ley General de Sanidad hasta la LOPD.

El artículo 23 de la Ley l4/l.986, de 25 de abril, General de Sanidad, autoriza, a la Administración Sanitaria, de acuerdo con sus competencias, para crear los Registros y elaborar los análisis de información necesaria para el conocimiento de las distintas situaciones de las que pueden derivarse acciones de intervención de la autoridad sanitaria.

Según el artículo 61 de dicha Ley el historial clínico sanitario, estará a disposición de los enfermos y de los facultativos que directamente estén implicados en el diagnóstico y tratamiento del enfermo, debiendo quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica.

Por el artículo 8 de la LORTAD y ahora de la LOPD se faculta a las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes para proceder al tratamiento de los datos de carácter personal relativo a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad, si bien, en la cesión de los mismos, no será preciso el consentimiento del afectado, conforme determina el apartado 2 letra f) del artículo ll, cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos, en los términos establecidos en la legislación sobre sanidad estatal o autonómica, necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria.

5.6.- Seguridad de datos

El artículo 9 de la LORTAD establecía una especial obligación del responsable del fichero,y, en su caso, la LOPD lo extiende, al encargado del tratamiento para garantizar la seguridad de los datos de carácter personal.

---

16 Belen Cardona, María, Datos Sanitarios del Trabajador: Límites a su utilización, Milán, Quadernin della Sezione di Teoria Generale e Informatica del Diritto, Año 1999.

El artículo 9 comprende tres apartados, que comprende dos ordenes de cuestiones: a) la obligación del responsable del fichero,y, en su caso, el encargado de tratamiento, de adoptar medidas de índole técnica y organizativas tendentes a garantizar la seguridad de los datos, y b) una habilitación reglamentaria para regular la seguridad de los ficheros.

El apartado 9.1[17] parece innecesario a la vista de los otros dos, puesto que es el Gobierno el que deberá determinar por vía reglamentaria las medidas de seguridad que deberá adoptar el responsable del fichero,y, en su caso, el encargado del tratamiento.

Coincidimos por Alvarez Cienfuegos[18] cuando dice que la culpa "in vigilando" del responsable del fichero se revela especialmente severa, pues la obligación de diligencia en la custodia se ha de adecuar al desarrollo de la tecnología (en constante y rapida evolución) y a la naturaleza de los datos almacenados.

Surgen así, para el responsable del fichero y, en su caso, el encargado del tratamiento, de una serie de obligaciones de carácter permanente que deberán ser vigiladas por la Agencia de Protección de Datos.

Los riesgos que puedan afectar a la seguridad de los datos de carácter personal están en dependencia directa del sector concreto donde se desenvuelva el fichero. Por ello y tratándose de conceptos jurídicos esencialmente indeterminados, susceptibles de ser modulados por el espacio y el tiempo no puede dictarse normas de aplicación general a todos los ficheros.

Confirmando la transcendencia de la custodia de los ficheros, locales, programas o equipos, que contengan datos de carácter personal, el artículo 44.3.h) califica de infracción grave la omisión de las medidas de seguridad que reglamentariamente se determinen.

5.7.- El deber de secreto

El artículo 10 de la LOPD estable que "el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo", artículo idéntico al contenido en la LORTAD a excepción la supresion de la palabra "automatizado" ya que, en la LOPD, ha desaparecido el termino automatizado de casi todos los lugares en los que se encontraban en la LORTAD,siendo ésta una cuestión muy significativa que da pie a múltiples interpretaciones y, cómo no, a elucubraciónes de todo tipo.

El artículo 10 deja claro y como obligacion elemental, el deber de secreto y el compromiso perdurable en el tiempo, incluso despues de finalizar las relaciones con el titular del fichero automatizado,pero ¿ Durante cúanto tiempo será exigible esta obligación de sigilo ?, desde luego mientros los datos puedan afectar a los derechos de la persona amparada por la protección de la Ley, pero variaran de un caso a otro según la naturaleza de los datos.

Merecen, en principio, el calificativo de infracciones muy graves, según el art. 44.4.g): "la vulneración del deber de guardar secreto sobre los datos de carácter persona a que hacen referencia los apartados 2 y 3 del art. 7", esto es, respecto de los datos especialmente protegidos por referirse a la ideología, afiliación sindical, religión y creencias, y los que hagan referencia al origen racial,a la salud y a la vida sexual.

También el art. 44.3.g) tipifica de infracciones graves otro tipo de vulneraciones al deber de guardar secreto sobre los datos de carácter personal,cuando no constituyan infracciones muy graves.

---

17 Heredero Higueras, Manuel, La Ley Orgánica, 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Caracter Personal, Madrid, Editorial Tecnos S.A, Año 1996, Pág. 113.

18 Alvárez-Cienfuegos Suárez, José María, La Defensa de la Intimidad de los Ciudadanos y la tecnología Informática, Pamplona, Aranzadi, Colección Divulgación Jurídica, Año 1999, Pág.39.

5.8.- Acceso a los datos por cuenta de terceros

La LOPD introduce en este título, el artículo 12, que no existia en la LORTAD, dedicado a los principios, el acceso a los datos por cuenta de terceros, no considerando cesión el acceso a los datos de un tercero cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento; se regula así, respecto al tratamiento de datos, la figura del encargado del tratamiento, que deberá tratar los datos de acuerdo con las instrucciones que le hubiere proporcionado el responsable del tratamiento, que deberan figurar en un contrato escrito o en alguna otra forma que permita acreditar su celebración y contenido y que estará obligado a implementar las medidas de seguridad a que se refiere el artículo 9 de la LOPD, al igual que a destruir o devolver al responsable del tratamiento los datos de caracter personal.

5.9 Comunicación de datos

El artículo 11, se dedica a la comunicación de datos (cesión de datos en la LORTAD).

El cambio terminológico, cesión de datos por comunicación de datos, y no en todas las ocasiones, sólo puede servir para sembrar confusión, pues no es bueno en unos artículos referirse a un concepto con un nombre para después referirse al mismo concepto en otro artículo con un nombre distinto.

En principio, y conforme al párrafo 1 del artículo 11, la comunicación de datos personales solamente puede producirse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

El consentimiento del afectado es básico para la cesión de datos. Se le ha de solicitar en términos concretos e informándole quién es el cesionario y la finalidad que se pretende con la cesión, de lo contrario sera nulo el consentimiento prestado.

Le es aplicable, a la cesión de datos, todo lo anteriormente, apuntado sobre el consentimiento.

Con la salvedad de los datos sensibles (art.7.3) y de los relativos a la salud (art.11.7), que requieren un régimen distinto para ser cedidos, la regulación o mejor dicho las excepciones contenidas en el número 2 del artículo 11 nos vuelven a poner de manifiesto que dicho artículo queda seriamente devaluado, al establecer que no será preciso el consentimiento, cuando una ley prevea otra cosa, o sean datos recogidos de fuentes accesibles al público; cuando el tratamiento -antes establecimiento del fichero automatizado- responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. Tampoco requerirá el consentimiento las cesiones de datos que tengan por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas.

Según este artículo, no será necesario el consentimiento del afectado, cuando la cesión se produzca entre las Administraciones Públicas y tengan por objeto el tratamiento posterior de los datos con fines históricos, estadístico científicos. Este punto e)2. del artículo 11, es más concreto que el de la LORTAD eliminado que los extendía a los supuestos previstos en el artículo 19.

6. DERECHOS DE LAS PERSONAS

Los aspectos principales de la posición de los ciudadanos a quienes pertenecen los datos a tratar informáticamente, se hallaban recogidos en el Título II y III de la LORTAD y ahora de la LOPD.

Los preceptos del Título II, como se desprende del apartado anterior, se dedicán más bien a definir el marco en el que han de moverse quienes deseen operar con datos de carácter personal y la forma en que pueden recoger-

los, tratarlos, conservarlos y cederlos, mientras que el Título III, al que vamos a dedicar este apartado, constituye el núcleo del sistema de garantías de la Ley y se centra en los derechos de las personas a impugnación, consulta, acceso, rectificación, cancelación, oposición, tutela e indemnización y se encuentra regulado en los artículos 13 a 19, ambos inclusive, de la LOPD, que completa los derechos tradicionales de acceso, rectificación y cancelación con los de oposición, impugnación, tutela y consulta que no contemplaba la LORTAD.

6.1.- Impugnación de valoraciones

El derecho de impugnación de valoraciones que en la LORTAD se refería a las producidas por un tratamiento automatizado, en la LOPD es más general, refiriendose a cualquier tipo de tratamiento.

La LOPD al igual que la LORTAD comienza su Titulo tercero con el reconocimiento de un derecho de gran transcendencia práctica: se establece una nueva acción, se legitima a los ciudadanos para impugnar - en términos de estricta técnica procesal ha de entenderse para recurrir demandando su invalidez - todo acto administrativo o decisión privada que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Al tratarse, según Alvarez-Cienfuegos[19], de una eventual lesión de un derecho que afecta a la intimidad de la persona, derecho fundamental reconocido en el art. 18.4 de la Constitución, nos encontramos ante una típica acción de nulidad que, a nuestro juicio, podrá ejercitarse en cualquier tiempo, no estando sujeta a plazo de prescripción o caducidad.

El punto 4 del art. 13 sienta un principio importante: "la valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado".

6.2 Derecho de consulta al registro general de protecciòn de datos

En nuestra época el poder que confieren las modernas tecnologías a los centros recolectores de información exceden los límites de lo imaginable.

Nuestros legisladores, conscientes de tal poder y su repercusión, introducen en el artículo 14 de la LOPD, el artículo 13 de la LORTAD que faculta a que "Cualquier persona pueda conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, su finalidad y la identidad del responsable del tratamiento".

Este derecho de información no es el adecuado, puesto que lo único que se concede es la facultad de conocer que ficheros existen, pero no en cuales se encuentra registrado el interesado y los datos que del mismo se contienen en cada uno. Este principio de información queda en la Ley sustituido, en este sentido, por el derecho de acceso, confundiendo ambos.

El supuesto contemplado en el artículo 14, va destinado a facilitar información sobre la existencia de ficheros de datos de carácter personal y sus finalidades, distinto al derecho a la información en la recogida de datos que reconoce el artículo 5 de la Ley.

Con el fin de facilitar este derecho se dispone, igualmente, que "El Registro General será de consulta pública y gratuita".

Poniendo en consonancia los dos preceptos citados nos encontramos que hay un derecho de información, previo a la recogida de los datos personales, acerca de la finalidad y el destinatario de la información que se reca-

19 Alvarez-Cienfuegos, José María, obra citada.

ba, así como de los derechos que, en general corresponden al afectado como consecuencia de la obtención de tales datos, y otro derecho de información que nos permitirá conocer, con posterioridad, la existencia de ficheros automatizados de datos de carácter personal.

6.3 Derecho de acceso.

El derecho de acceso, recogido en el artículo 15 de la Ley, otorga al afectado la facultad de solicitar y obtener información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos, tiene incluso plasmación constitucional, pues esta facultad aparece reconocida no con el rango de derecho fundamental, pero sí como derivación del derecho a recibir libre información en el artículo 105.b de la Constitución.

Por medio del derecho de acceso la persona tiene la facultad de conocer la información que le concierne y controlarla mediante el derecho de rectificación y cancelación.

Podemos considerar el derecho de acceso como el eje del sistema de garantías arbitrado por la Ley, ya que faculta a su titular o el legitimado para ello para exigir el conocimiento preciso de los datos de carácter personal que se incluyan en un fichero automatizado.

La información podrá consistir en la mera consulta de los datos en la LOPD -ficheros en la derogada LORTAD- por medio de su visualización, o la indicación de los datos que son objetos de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos especiales (art.15.2).

El derecho de acceso se ve limitado, en el tiempo, pues, conforme al apartado 3 del artículo 15, este derecho se puede ejercitar en plazos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Las excepciones, a este principio, son generosas y se consagran, básicamente, en los artículos 22 y 23, para ficheros de titularidad pública (Fuerzas y Cuerpos de Seguridad del Estado, Hacienda Pública...), cuyo acceso queda indeterminado, mientras el acceso cobra plena efectividad en el campo de los ficheros de titularidad privada.

La ley, en su artículo 17, nos indica que el procedimiento para ejercitar el derecho de oposición, acceso, así como el de rectificación y cancelación serán establecidos reglamentariamente, esperemos que sean desarrolladas cuidadosamente, si bien consideramos debería regularse por Ley con el fin de ofrecer mayores garantías. El artículo 24.2 de la LOPD, establece que si el órgano administrativo dicta resolucion negativa instruirá al afectado del derecho que le asiste de dirigirse a la Agencia de Protección de Datos, o en su caso, del órgano equivalente de las Comunidades Autónomas, para terminar, si fuese necesario, en los Tribunales de Justicia.

Por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación de los datos de carácter personal inexactos no se exigirá contraprestación alguna, según el art. 17.

6.4 Derecho de rectificacion y cancelacion

El derecho de rectificación y cancelación, unidos a los derechos de información - ahora denominado derecho de consulta al registro general de protección de datos -, impugnación, oposición, acceso e indemnización constituyen el núcleo del sistema de garantías previstos en la Ley y recogidos en los artículos 13 a 19, derechos, algunos a los que la exposición de motivos de la LORTAD quiso destacar cuando dice: "los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado en la Ley".

El artículo 16 sólo prevé que, cuando resulten no ajustados a lo dispuesto en la LOPD, inexactos o incompletos, los datos de carácter personal, serán rectificados y cancelados en su caso, pero se deja para su regulación reglamenta-

ria el procedimiento para ejercitar el derecho de oposición, acceso, rectificación y cancelación en su caso.

Del párrafo precedente parece deducirse que siempre que haya un dato inexacto éste deberá cancelarse, de oficio o a instancia de parte.

El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación en el plazo de 10 días.

Siguiendo a Velázquez Bautista[20] diremos que la actualización de la información es una de las obligaciones del creador o gestor de la base de datos, forma parte de su trabajo, se halla directamente relacionado con la calidad del fichero, deberá cumplirse de oficio. Aunque esto no es óbice para que la actualización de los datos se plantee a partir del ejercicio del Derecho de acceso.

La rectificación, aunque pueda entenderse como una forma de actualizar los datos, no hay que considerarla como una actividad equivalente. Pues, mientras la rectificación presupone la existencia de unos datos erróneos, la actualización es una puesta al día de éstos, no porque los anteriores fueran incorrectos o erróneos, sino por que se han quedado desfasados.

Así, en el caso de rectificación sustituimos datos erróneos por información cierta o sin error, mientras en la actualización no hay por que sustituir información pues la misma no era errónea, sino que se ha quedado desactualizada.

Según esto, quedan registrados sin modificarse los datos anteriores mientras se añaden unos datos nuevos gracias a los cuales se pone al día la información.

El derecho de rectificación aparece ya recogido en el artículo 8 del Convenio 81 del Consejo de Europa, así como en el art. 16 de la propuesta de Directiva Comunitaria, en forma similar al art. 15 de la LORTAD. De todos ellos se deduce que la posibilidad de que se rectifiquen los datos forma parte del mínimo necesario que deben contener las leyes de protección de datos, asimismo supone una consecuencia lógica del ejercicio del Derecho de acceso pudiendo afirmarse, que es una de sus finalidades

La rectificación y cancelación de los datos es una obligación que tienen los responsables del tratamiento, cuyo incumplimiento supone una infracción de la norma para la protección de datos, incluida entre las infracciones graves, en el art. 44.3.f) de la Ley y sancionadas conforme al art. 45.3 con multa de 10.000.001 a 50.000.000 de pesetas, más la indemnización que corresponda por la reclamación de daños y perjuicios que se pudiese exigir, ante los órganos de la jurisdicción ordinaria, si los ficheros fuesen de titularidad privada, en base al artículo 1902 del Código Civil y 19 de la LOPD (antes 17.3 de la LORTAD), por los causados como consecuencia del incumplimiento de lo dispuesto en la presente Ley. Si los ficheros fuesen de titularidad pública la via será la contencioso-administrativa.

Si los datos no fuesen pertinentes o adecuados a la finalidad que originó su registro, o pertenecen a la esfera privada del sujeto en tal grado que éste no desea que se registren, y no viene obligado a ello, o hubiese revocado su autorización para que sean incorporados al fichero, podrá, si no se hubiese hecho de oficio, ejercitar su derecho de cancelación exigiendo se borren o bloqueen tales datos.

Igualmente deberán ser cancelados los datos de carácter personal cuando finalice su periodo de vida o como dice el art. 4.5 "los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados". La extensión de la duración guarda, conforme al núm. 5 del art. 15, relación con el fin para el que se obtuvieron, así como con lo que dispongan las disposiciones legales. Una serie de informaciones sobre las personas seguirán vivas incluso después del fallecimiento: ejemplo las inscripciones de nacimiento, matrimonio y defunción del Registro Civil, otras, del mundo empresarial

20 Velázquez Bautista, Rafael, Protección Jurídica de Datos Personales Automatizados, Madrid, Colex, Año 1993.

y por mandato del art. 45 del Código de Comercio, deberán conservarse durante cinco años, en otros su duración podra ser fijada a priori y en otros no, pero en todos casos procede su cancelación.

Tema polémico ha sido la expresion "cancelar" de la LORTAD, pues para unos significaba borrar, para otros anular, hacer ilegibles, destruir, dejar irreconocible, dejar nulos, etc, se decía que sería conveniente definir, a efectos de la LORTAD, qué se entiendía por cancelar y la LOPD en el artículo 16.3 nos dice que la cancelación dará lugar al bloqueo de los datos conservandose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de estas. Cumplido el citado plazo deberá procederse a la supresión.

La figura del bloqueo, por fín tiene su respaldo en la LOPD más concretamente en el artículo 16.

Otro tema conflictivo puede ser la rectificación o cancelación de los datos cedidos al extranjero, por la dificultad que, en algunos casos, puede entrañar hacer realidad tal derecho.

Las actuaciones contrarias a la presente Ley pueden ser objeto de reclamación, por los afectados, ante la Agencia de Protección de Datos y contra las resoluciones de éstas procederá recurso contencioso-administrativo (art. 17).

Para concluir, con el Título III, diremos que es clave en esta Ley, el derecho de las personas a acceder a los datos poseidos sobre ellos y controlar su posible divulgación.

Se trata por tanto de que la persona conozca y disponga de posibilidades reales de acceder a las informaciones que sobre ellos obran en manos de terceros, y se encuentran archivadas en bancos de datos. El consentimiento y acceso a la información es una garantía indispensable que debe reconocerse y tratarse jurídicamente.

La aparición de nuevas necesidades humanas, así como nuevas modalidades de amenaza y formas de agresión de las libertades, exigen ser tenidas en cuenta y remediadas.

El Habeas Data, según Pérez Luño,[21] constituye, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática, y cumple una función paralela al Habeas Corpus respecto a la libertad física o de movimiento de la persona.

No es dificil establecer un marcado paralelismo entre la "facultad de acceso" a las informaciones personales que conciernen a cada ciudadano, en que se traduce el habeas data, y la acción exhibitoria del habeas corpus.

El Habeas Corpus surge como replica frente a los fenómenos abusivos de privación de la libertad física de la persona, propio en la antigüedad y medievo y llegando a la actualidad con los regimenes totalitarios. El Habeas Corpus aparece como un recurso procesal por el que se solicita del Juez que se dirija al funcionario que tiene una persona detenida y la presente ante él. Se trata, por tanto, de una garantía judicial específica para la tutela de la libertad personal.

La aparición del Habeas Data no puede entenderse como una sustitución del Habeas Corpus, cuya función para la defensa de la libertad física sigue siendo plenamente vigente, sino que se trata de una garantía para nuevas agresiones a otras facetas de la libertad (la identidad de la persona, su autodeterminación, su intimidad.....).

6.5 Procedimiento.

Junto al acceso, el individuo debe controlar la calidad de los datos almacenados en ficheros electrónicos, a fin de poder, en su caso, rectificar o cancelar los datos inexactos o indebidamente procesados, al igual que debe disponer sobre su transmisión.

---

[21] Pérez Luño, Antonio Enrique, "Del Habeas Corpus al Habeas Data", UNED MERIDA, Informática y Derecho, Vol. Nº 1, Año 1992.

Para la efectividad de lo anterior hace falta un procedimiento que la Ley pospone a una decisión reglamentaria, no sólo del procedimiento para ejercitar el derecho de acceso, rectificación o cancelación, sino tambien, para las reclamaciones ante la Agencia de Protección de Datos. En cualquier caso la reclamación previa ante la Agencia de Protección de Datos parece obligado según la relación del artículo 18 de la LOPD.

Siguiendo a la Profesora Gayo Santa Cecilia[22], en cuanto al tratamiento específico que la LORTAD contiene en relación con la protección de los derechos de información, acceso, rectificación y cancelación, parece claramente insuficiente, no sólo por dejar en manos de la Agencia de Protección de datos, un órgano administrativo, la competencia para conocer y resolver las reclamaciones, pues consideramos que quizas un órgano judicial podría haber resultado más eficaz para resolver los posibles conflictos de intereses que surjan, más aun cuando la actuación ante la que se pretende reclamar ha sido realizada por la propia Administración pública; sino sobre todo por no concretar un procedimiento específico para su resolución.

Con todo se ha introducido una posible intervención de los órganos jurisdiccionales al hacer referencia el artículo 18.4 de la LOPD a la hipotética procedencia de un Recurso Contencioso-Administrativo contra las resoluciones de la Agencia de Protección de Datos, si bien surge la duda acerca de a qué tipo de Recurso Contencioso-Administrativo se está haciendo referencia, si al contenido en la Ley Reguladora de la Jurisdicción Contencioso-Administrativo o al regulado en la Ley 62/1978 de 26 de diciembre de protección jurisdiccional de los derechos fundamentales de las personas, ya que, en el caso de que dicho recurso haya de tramitarse por la via contencioso-administrativa, la obtención de una resolución definitiva podría prolongarse excesivamente, lo que nuevamente supondría un menoscabo de los derechos y libertades de los ciudadanos.

El mismo resultado se produce en relación al Derecho a ser indemnizado del art. 19.3, tanto por la existencia de una duplicidad de regulaciones según se trate de ejercitarlo ante las Administraciones Públicas o ante sujetos privados, como por la elección de los órganos de la jurisdicción ordinaria como vía de salvaguarda de los derechos en el segundo de los supuestos, puesto que los procedimientos que se pueden instar ante dicha jurisdicción son largos y complejos, lo que podría llegar a desvirtuar la finalidad protectora que se pretende.

La disposición adicional 4ª de la nueva ley de la jurisdicción contencioso-administrativa, Ley 29/1998, de 13 de julio, atribuye competencia para conocer de los recursos contra los actos administrativos y disposiciones generales de la Agencia de Protección de Datos a la Sala de lo Contencioso Administrativo de la Audiencia Nacional.

7. LOS FICHEROS

Entre las principales novedades que trae la LOPD con respecto a la LORTAD es la inclusión en el ámbito de protección de la ley de todos los ficheros de datos, informatizados o no, de aquí la supresión del término automatizado que seguía al término fichero.

La LOPD al igual que hacía la LORTAD, después de sentar los que ella llama principios y derechos de las personas en sus Títulos II y III, respectivamente, dedica el Título IV a lo que define como "disposiciones sectoriales", con dos capítulos, el primero de ellos, con cinco artículos del 20 al 24, dedicado a los ficheros de titularidad pública y el segundo, con ocho artículos del 25 al 32, dedicado a los ficheros de titularidad privada.

Conforme hemos apuntado, con anterioridad, la propia exposición de motivos de la LORTAD nos indicaba que la Ley se nuclea en torno a los que convencionalmente se denominan "ficheros de datos", a tal efecto la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica, dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo, como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia.

22 Gayo Santa Cecilia, Mª. Eugenia, "Garantías del ciudadano ante la L.O.R.T.A.D.: Posibles Vías de Defensa y Protección de sus Derechos Fundamentales", UNED MERIDA, Actas III Congreso Iberoamericano de Informática y Derecho, Año 1992.

UNIVERSIDAD BIBLIOTECA DE LIMA

En las disposiciones generales de la LOPD se dedica el artículo 3 a una serie de definiciones y entre ellas el apartado b) nos lo hace de los ficheros como: "Todo conjunto organizado de datos de carácter personal cualquiera que fuese la forma o modalidad de su creación, almacenamiento, organización y acceso".

El concepto informático de fichero no se corresponde con el concepto jurídico, por lo que a efectos de notificación, toda una base de datos (definida en el artículo 12 de la Ley de Propiedad Intelectual, como la sistematización y/o recopilación de datos), compuesta por múltiples ficheros informáticos, puede ser tratada como un único fichero jurídico.

Si acudimos a los artículos 9 y 10, relativos al secreto profesional y seguridad de los datos, donde se habla del responsable del fichero, sin distinción de público o privado, podría llevarnos a la conclusión de que las normas contenida en esta Ley rigen por igual para todos, cualquiera que sea su naturaleza. El análisis del presente título nos pone de manifiesto que esto no es así, pues no sólo se ha definido un régimen jurídico distinto para unos y otros, sino que, respecto a los ficheros de titularidad pública, se ha introducido, en casos señalados, notorias restricciones al ejercicio de los derechos de información, acceso, rectificación y cancelación.

7.1 Ficheros de titularidad publica

A ellos se dedica, como ya hemos indicado, el Capítulo Primero, del Título IV en sus artículos 20 a 24, ambos inclusive, y comienza diciéndonos que su creación, modificación o supresión de los ficheros de las Administraciónes Públicas sólo podran hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente y en la que deberá indicar: la finalidad, las personas sobre las que se pretende obtener los datos, el procedimiento de recogida, la estructura básica, las cesiones, los responsables del fichero, las medidas de seguridad...

Para dar cumplimento al artículo 20 los órganos de gobierno de los Poderes e Instituciones públicas, en el ejercicio de sus competencias y en el ámbito de su propia organización deberán adoptar un acuerdo -de indudable matíz reglamentario- por el que se decida crear, modificar, o estinguir el oportuno fichero de datos, con las especificaciones del citado artículo 20.

Las excepciones, hacen pensar que existen limitaciones en el ejercicio de los derechos reconocidos a los ciudadanos, cuando se trata de ficheros de titularidad pública, pues ellas permiten la cesión de datos de carácter personal, en determinadas circunstancias, entre Administraciones Públicas, e incluso la recogida y tratamiento automatizado por las Fuerzas y Cuerpos de Seguridad, sin consentimiento de las personas afectadas, de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, esto es, los que se han dado en llamar "datos sensibles".

Algunas de las excepciones contenidas en los artículos 21, 22, 23 y 24 suponen un grado de indeterminación y un vacío que permite el discrecional uso de las limitaciones enunciadas en la Ley, según la cual sólo podrán establecerse excepciones cuando ponderados los intereses en juego, valorados los peligros potenciales de una y otra opción, deba entenderse que es más grave para el orden constitucional informar al afectado, o permitirle el acceso y rectificación, que negarle el uso de estas facultades.

Las excepciones contenidas en los artículos 23 y 24 hacen referencia, no sólo, a los derechos de acceso, rectificación y cancelación, sino también, a los de información en la recogida de datos y a la privación del consentimiento del afectado.

7.2 Ficheros de titularidad privada.

Mayor número de artículos dedica la Ley a los ficheros de titularidad privada, del 25 al 32, ambos inclusive, que son los que constituyen el capítulo II del Título IV, y en ellos se trata: la creación, notificación e inscripción registral, comunicación de la cesión de datos, datos incluidos en las fuentes de acceso al público, prestación de ser-

vicios e información sobre solvencia patrimonial y crédito, ficheros con fines de públicidad y prospección comercial, censo promocional y Códigos tipo.

En los ficheros de titularidad privada, se exige siempre el consentimiento del interesado para recabar los datos, consentimiento, que como hemos apuntado anteriormente, puede ser revocado, pero sin producir efectos retroactivos.

En la cesión de datos, también, es necesario el consentimiento del afectado, que deberá, igualmente, ser informado, por el responsable del fichero, en el momento en que se efectue la primera cesión de datos.

Tienen plena efectividad los derechos de información, acceso, rectificación y cancelación, así como de cuantas garantías, esta Ley, reconoce a los ciudadanos y que en los ficheros de titularidad privada adquieren plena efectividad, por lo que no es necesario repetir lo que sobre cada uno de ellos hemos apuntado anteriormente.

Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará "previamente" a la Agencia de Protección de Datos, haciendo constar, además de lo que reglamentariamente se establezca, el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones que se prevean. Tras la notificación a la Agencia, pueden darse dos supuestos: que la Agencia de Protección de Datos resuelva o que deje transcurrir el tiempo sin resolver.

En caso de resolución, ésta, corresponde, en base al artículo 12.2.a), del Real Decreto 428/l.993, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, al Director de la Agencia de Protección de Datos y debera ser motivada sobre la procedencia o improcedencia de la inscripción en el Registro General de Protección de Datos; con su decisión se agota la via administrativa, contra la que cabe recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, según el artículo 18.4 de la Ley y art. 2.4 del Estatuto de la Agencia de Protección de Datos y la Ley 29/1998 de la Jurisdicción Contencioso-Administrativo.

Si no hubiese resolución, transcurrido un mes desde la presentación de la solicitud de inscripción, sin que la Agencia de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos (art. 26).

Según la disposición adicional primera de la Ley los ficheros y tratamientos automatizados, inscritos o no, en el momento de entrada en vigor de la presente Ley, deberán adecuarse a la LOPD dentro del plazo de tres años.

Los ficheros y tratamientos no automatizados, su adecuación a la LOPD deberá cumplirse en el plazo de 12 años a contar desde el 24 de octubre de 1995.

Los responsables de ficheros de titularidad pública y privada podrán formular códigos tipo que establezcan las condiciones de organización, funcionamiento, procedimiento, normas de seguridad, programas, obligaciones..., que tendrán el carácter de códigos deontológicos o de buena práctica profesional y que deberán ser depositados o inscritos en el Registro General de Protección de Datos.

En las líneas precedentes hemos apuntado las principales reglas comunes a todo fichero de titularidad privada, que recoge el capítulo II, en el que a su vez aparecen una serie de disposiciones que se refieren a aspectos singulares de los que se ocupan de unas determinadas finalidades, como a solvencia patrimonial, publicidad, encuestas o investigaciones...

Una importante novedad de la LOPD es la creación del "Censo Promocional" al que se refiere el art. 31 en el que se recogerán los nombres, apellidos y domicilio del censo electoral de aquellos ciudadanos que no se hayan opuesto a figurar en aquel.

Este precepto hará posible el Censo promocional y su utilización cosa que hasta ahora era imposible, pues la Junta Electoral Central se había pronunciado al respecto en el sentido de que los datos de ciudadanos que constan en el Censo Electoral sólo tiene por misión el facilitar a aquellos el derecho de sufragio activo, no pudiendo ser empleados para otros usos, a excepción de su cesión a los Tribunales. El nuevo Censo promocional parece que vendrá

a solucionar este problema sin mermar el derecho de los ciudadanos a decidir que sus datos se usen o no para aquellos fines. Reglamentariamente se regulará el procedimiento mediante el que los interesados podrán solicitar no aparecer en el Censo promocional.

8. MOVIMIENTO INTERNACIONAL DE DATOS

El título V de la LOPD, bajo el epígrafe de "movimiento internacional de datos" comprende los artículos 33 y 34 y regula la transferencia de datos transfronteras y sus requisitos, de acuerdo con la protección existente en el destino, que debe ser equiparable al que presta la presente Ley (art. 33).

En este punto, como en otros de la LORTAD y la LOPD, hay una terminología distinta en la exposición de motivos de la LORTAD, donde se habla de "transmision internacional de datos", "flujo internacional de datos", para utilizar en el artículado la expresion "transferencia" y enunciar el capítulo con el de "movimiento internacional de datos".

Se pone en manos del Director de la Agencia de Protección de Datos el determinar qué entiende por equiparable y por tanto si hay o no garantía, en otros paises, para transmitir los datos de carácter personal.

En los dos artículos, que regulan la materia, no aparece epígrafe alguno destinado a regular la importación de datos personales de otros paises.

El artículo 34 de la LOPD amplia las excepciones de la LORTAD, y regula, una vez más, una serie de excepciones, tales como: cuando resulte de tratados o convenios; a efectos de prestar o solicitar auxilio judicial internacional; de datos de carácter médico entre facultativos o instituciones sanitarias; o cuando se refiera a transferencias dinerarias, cuando el afectado haya dado su consentimiento...

9. AGENCIA DE PROTECCION DE DATOS

Como Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada,se regula, en el Titulo VI de la LORTAD, artículos 35 a 42, el órgano de fiscalización y control bajo el nombre de Agencia de Protección de Datos.

El título VI de la Ley Orgánica 5/1992, crea la Agencia de Protección de Datos que mantiene la LOPD y dispone, en su artículo 35, que se regirá, fundamentalmente, por lo dispuesto en dicha Ley y en un Estatuto propio que será aprobado por el Gobierno.

Por Real Decreto 428/1993, de 26 de marzo, se aprueba el Estatuto de la Agencia de Protección de Datos, que seguirá subsistente por mandato de la disposición transitoria 3ª de la LOPD hasta tanto, conforme a la disposición final primera, el Gobierno apruebe uno nuevo o lo modifique.

Tiene como misiones primordiales velar por el cumplimiento de la Ley, dictar instrucciones, sancionar las infracciones de caracter administrativo previstas en ella, atender las reclamaciones de los interesados, y redactar la memoria anual...

En la estructura orgánica, de la Agencia de Protección de Datos, destaca la figura del director de la misma que será nombrado por Real Decreto, de entre quienes componen el Consejo Consultivo, por un período de cuatro años.

Al Director, órgano unipersonal, le corresponde la representación de la Agencia de Protección de Datos y, en exclusiva, las facultades ejecutivas y la suprema capacidad de decisión dentro de la Agencia, asistido por un Consejo meramente consultivo. Puede decirse, por ello, que la Agencia es el Director, toda vez que la función asesora del Consejo Consultivo sólo se ejerce a instancia del Director, sin perjuicio de formular propuestas en temas relacionados con las materias de la competencia de la Agencia (art. 18 del Estatuto).

No obstante destacar la exposición de motivos de la LORTAD la absoluta independencia del Director, lo cierto es que el mismo es nombrado por el ejecutivo a quien también corresponde su cese, a diferencia de lo que es norma habitual del derecho comparado, que lo nombra el Parlamento, por lo que se ha puesto en duda su absoluta independencia.

El Director permanece en el cargo por un plazo de cuatro años, al igual que los vocales del Consejo Consultivo. Su inamovilidad, durante este período, y el establecimiento, en el artículo 15 del Estatuto, de forma tasada, las causas de cese o separación del Director ha dejado de ser éste uno de los aspectos más controvertidos de la Ley, si bien al ser una de las causas "el incumplimiento grave de las obligaciones del cargo", circunstancia por completo carente de la certeza y concreción necesaria, pone en duda su absoluta independencia.

Según el artículo 2 del Estatuto, los actos del Director se consideran actos de la Agencia y agotan la via administrativa, no están sujetos, por tanto, a modalidad alguna de tutela administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

El Consejo Consultivo está integrado por nueve miembros propuestos uno por cada una de las siguientes instituciones: Congreso de los Diputados, Senado, Administración Central, Autonómica, Local, Universidad, usuarios, Academia de la Historia y un representante del sector de ficheros privados.

Junto al Director y Consejo Consultivo, la estrutura de la Agencia se completa, según el art. 11 del Estatuto, con el Registro General de Protección de Datos -donde serán objeto de inscripción, los ficheros automatizados de que sean titulares las Administraciones Públicas, los ficheros privados, las autorizaciones y los códigos tipo (art. 32 de la Ley)- la Inspección de Datos y la Secretaría General, como órganos jerárquicamente dependientes del Director de la Agencia.

Acogiéndose al artículo 40 de la LORTAD, que permite la asignación de competencias a las comunidades autónomas, a iniciativa de la Comisión de Libertades e Informática de la Comunidad Valenciana (CLIVA), el Magistrado Jesús Martínez Arenas, ha elaborado una propuesta de Ley Autonómica de Regulación del Tratamiento Automatizado de Datos de Caracter Personal, ya que según el Sr. Martínez Arenas "es necesario extender la Ley al ámbito autonómico porque existen marcos de legislación propios a los que no tiene acceso la Administración Central y donde se produce la utilización de datos de los ciudadanos".

La Agencia de la Comunidad de Madrid es, en este momento, la única agencia autonómica. Entiende su trabajo como un refuerzo de la autoridad de control nacional, que es la Agencia de Protección de Datos del Estado, como apoyo a su trabajo de cohesión y armonización en la aplicación de la ley en todo el estado, máxima autoridad, por tanto, en la materia.

10. INFRACCIONES Y SANCIONES.

Las sanciones administrativas cierran todo el sistema de garantías.

La LOPD no tipifica unos delitos por lo que en orden a las sanciones penales de la violación de los Datos de Carácter Personal hay que remitirse a los preceptos del Código Penal que como decíamos[23] para el legislador no existe un delito informático pero si una realidad criminal compleja que sanciona entre otras en los artículos 197 y ss. (atentandos contra la intimidad), 270 y ss. (propiedad intelectual), 278 y ss. (espionaje informático), 239, 248.2, 256.2, 264.2, 623.4...

Al título VII bajo el epígrafe "Infracciones y Sanciones", se dedican los artículos 43 a 49, en los que se trata: responsable, tipo de infracciones, tipo de sanciones, infracciones de las Administraciones Públicas, prescripción, procedimiento sancionador y potestad de inmovilización de ficheros.

---

[23] Carrascosa López, Valentín, "¿Es necesaria una legislación mundial para Internet?, UNED MERIDA, Informática y Derecho - Revista Iberoamericana de Derecho Informática, Vol. Nº 27-29, Año 1998, Pág. 178.

Tras establecer el artículo 43 que los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley, ésta, tras clasificar las infracciones en leves, graves y muy graves, describe,en el artículo 44, hasta un total de veintiseis infracciones, ampliables a cualquier otra, que se pueda incluir,en las concepciones muy amplias, que a las mismas dan los apartados, 3.d) y 4,f) del artículo 44.

La protección de la intimidad en relación con los datos, se sustenta, en la LOPD, sobre todo en el reconocimiento del carácter reservado de los mismos, lo que conduce a la consagración específica del deber de secreto (artículos 10 y 40.2) y el establecimiento de infracciones relativas al incumplimiento de tal deber, como grave (art. 44.3.g) o muy grave (art. 44.4.g).

También los tipos de infracciones pretenden proteger los derechos de información, acceso, rectificación y cancelación, movimiento internacional de datos, cesión, calidad de datos, consentimiento, datos especialmente protegidos, creacion de ficheros...

La cuantía, de las sanciones previstas, se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia (art. 45.4).

Las sanciones previstas, en el art. 45, son pecuniarias y afectan a los encargados de los tratamientos y a los responsables de los ficheros privados, con multa que va de:

100.000 a 10.000.000 para las infracciones leves
10.000.001 a 50.000.000 para las infracciones graves
50.000.001 a 100.000.000 para las muy graves

El tope mínimo, 100.000 pesetas, nos parece excesivo, al igual que bajo, el tope máximo, por infracciones muy graves, que, por otra parte, queda ponderado al disponer, el art. 49, que en los supuestos, constitutivos de infracción muy grave, -de utilización o cesión ilícita de los datos de carácter personal en el que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las Leyes garantizan- el Director de la Agencia de Protección de Datos, podrá requerir a los responsables del fichero de datos de carácter personal a la cesación en la utilización o cesión lícita de los datos y si este requerimiento fuese desatendido, podrá, mediante resolución motivada, inmovilizar tales ficheros, tanto públicos como privados, a los solos efectos de restaurar los derechos de las personas afectadas.

El sistema de sanciones de los artículos 44 y 45 sólo afecta a los titulares de ficheros privados, pues como dice Heredero Higueras[24], no tendría carácter disuasorio alguno imponer sanciones pecuniarias a un órgano de una Administración Pública, pues la sanción se resolvería en una adscripción o transferencia a favor del Tesoro, de parte de un crédito del presupuesto del órgano que incumpliera la Ley. Por ello, el artículo 46 prevé un sistema más directo, consistente en ordenar la cesión de un tratamiento de datos que incumpla la Ley y, en su caso, instar actuaciones disciplinarias contra el personal correspondiente.

La potestad sancionadora se encomienda a la Agencia de Protección de Datos, contra cuyas resoluciones, como ya hemos indicado, procederá recurso contencioso-administrativo.

Una vez más, la Ley, en su artículo 48, fija que por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de sanciones a que hace referencia el presente título.

[24] Heredero Higueras, Manuel, "La Ley Orgánica 5/1992, de 29 de Octubre, de Regulación Del Tratamiento Automatizado de los Datos de Carácter Personal", Madrid, Boletín de información del Ministerio de Justicia, Nº 1669, Año 1993.

II. LAS PRINCIPALES NOVEDADES DE LA LOPD, SI LA COMPARAMOS CON LA LORTAD

La transposicion, en su totalidad, de la Directiva no se hace en el plazo que la misma establecía para ello, pero incorpora la LOPD los principales principios de la Directiva que no habían podido ser recogidos, en su integridad, por la LORTAD, que si por el contraría habia recogido los importantes trabajos previos para llevar a término la que despues sería la Directiva 95/46/CE, y por ello la LORTAD se convirtio en una de las Leyes más protectoras del derecho a la intimidad de los ciudadanos ante los tratamientos informatizados de sus datos personales de todas las existentes en la Unión Europea, pero que ahora ha mejorado, en algunos aspectos, la LOPD y por eso vamos a recoger aqui las principales novedades que trae la LOPD, si la comparamos con la LORTAD y que podemos sintetizar en los siguientes párrafos:

1.- El nuevo texto no se ha limitado a la adecuación de nuestro ordenamiento a la Directiva, sino que también ha introducido modificaciones de gran calado, al aprobarse una nueva Ley que no se ha limitado a la transposición de la Directiva.

2.- La nueva Ley da un mayor rigor en la protección del derecho a la intimidad de los ciudadanos ante el tratamientos de sus datos personales.

3.- La nueva Ley al carecer de exposición de motivos, no va a estar exenta de dificultades.

4.- Se amplia el objeto de la Ley al incluir en el ámbito de protección de la Ley todos los ficheros de datos, informatizados o no, al propio tiempo que ahora se protege el tratamiento de datos personales respecto del conjunto de libertades públicas y derechos fundamentales de las personas y, especialmente, en el ámbito de su intimidad.

5.- En la LOPD ha desaparecido el término "automatizado" de casi todos los lugares en los que se encontraba en la LORTAD, aunque sobreviven algunos conceptos informáticos.

6.- Los derechos de los ciudadanos, hasta ahora circunscritos a los de acceso, rectificación y cancelación de sus datos, se ven completados con el derecho de oposición, con lo cual se viene a posibilitar que el posible tratamiento de datos no llegue a producirse.

7.- Se refuerza el consentimiento de los ciudadanos para que sus datos puedan ser tratados, consentimiento definido por la Ley que ahora exige sea libre, inequívoco, específico e informado.

8.- La nueva Ley define y delimita no sólo la figura del responsable del fichero o tratamiento - que decide sobre la finalidad, contenido y uso del tratamiento - sino también la del encargado del tratamiento -que trata datos personales por cuenta del responsable del tratamiento-.

9.- La nueva Ley delimita, en las definiciones, el concepto de "fuentes de acceso al público", indicando que fuentes tienen, exclusivamente, la consideración de accesibles al público: el censo promocional -una importante novedad de la LOPD-, repertorios telefónicos, listados de profesionales publicados, diarios y boletines oficiales y medios de comunicación.

10.- Reforzamiento de la finalidad de los datos, pues su fin no solo debera ser legítimo, como exigia la LORTAD, sino tambien determinado y explícito.

11.- En el artículo 4.2, de la LOPD, se produce el cambio de una palabra que puede tener gran importancia a la hora de la aplicación práctica, pues mientras las LORTAD decía "no podrá usarse para "finalidades distintas", la LOPD no habla de finalidades distintas sino de "finalidades incompatibles".

12.- Mejora la garantía de los ciudadanos al derecho a la información previa, sin excepción alguna, a la recogida de datos y la exigencia de información al interesado, dentro de los tres meses siguientes a su registro, cuando los datos no han sido recabados del mismo.

13.- Destacar que, siguiendo la doctrina del Tribunal Constitucional,los datos sindicales se incorporan entre los especialmente protegidos.

14.- El cambio del término cesión de datos por comunicación de datos, y no en todas las ocasiones, sólo puede servir para sembrar aún más confusión a la hora de aplicar la Ley

15.- En la cesión de datos se introduce como nuevas excepción la comunicación que tenga por destinatario el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.

16.- Se conservan en forma parecida, el derecho de información, acceso, y los derechos de rectificación y cancelacion, pero se introduce en el de cancelación, la figura del bloqueo de los datos.

17.- Se clarifican mejor determinadas exigencias, se concreta la procedencia de los datos que pueden incorporar y se establece alguna precisión para quienes se dediquen a la prestación de servicios de información sobre solvencia patrimonial y de crédito.

18.- El tratamiento con fines de publicidad y de prospección comercial se conserva pero con algunas modificaciones.

19.- En los códigos tipo la LOPD amplía la posibilidad de establecer los mismos a los ficheros de titularidad pública y así como las organizaciones que se agrupen.

20.- Respecto a infracciones y sanciones, cabe destacar una mejor concreción y la posibilidad de rebaja económica, excepcionalmente, al permitir establecer la cuantía de la sanción aplicando la escala relativa a la clase inmediata inferior en gravedad.

Podemos concluir diciendo con Eugenio Díaz que por lo que se refiere a las particularidades de la violación de la intimidad en Internet hay que resaltar estos dos puntos: primero, que rigen en el ciberespacio tanto las disposiciones de la LORTAD, ahora la LOPD, sobre Protección de Datos de Carácter Personal como las del Código penal en Materia de ilícitos penales informáticos: segundo, que la información de Carácter Personal que salta a la red por libre decisión de su titular debe entenderse que no tiene carácter privado sino público, si bien la información residente en el disco duro del ordenador no puesta a disposición del público, debe entenderse como información reservada, de modo que quienes la observen transmitan o manipulen invaden ilícitamente la intimidad ajena.[25]

[25] Eugenio Díaz, Francisco, "La Protección de la Intimidad y el uso de Internet", UNED MERIDA, Informática y Derecho - Revista Iberoamericana de Derecho Informático, Vol. Nº 30-32, Año 1999, Pág. 171.

La Protección del Derecho a la Intimidad y Privacidad frente a las Nuevas Tecnologías

Aldo Antonio Elliot Segura (Perú)
aelliot@olemail.com

1. CURRICULUM VITAE

- Abogado, egresado de la Facultad de Derecho y Ciencias Políticas de la Universidad de Lima en 1997.

- Máster en Informática y Derecho, graduado en 1999 y llevado a cabo en la Universidad Complutense de Madrid-España, cuyo Director es el Prof. Emilio Suñé Llinas.

- Ha realizado labores en el Ministerio de Energía y Minas en Lima y ha colaborado en la Agencia de Protección de Datos de la Comunidad de Madrid, así como en la revista española especializada en informática "MasPC".

- Ha demostrado desde sus estudios de Pre-grado gran interés por los temas de Derecho Informático e Informática Jurídica, los cuales quiere profundizar y sobretodo desarrollar en la medida de lo posible.

2. RESUMEN DE PONENCIA

La legislación en materia de protección de datos con el reconocimiento de nuevos derechos para los ciudadanos es un tema novedoso y de gran importancia en estos momentos.

La regulación sobre tratamiento automatizado de datos de carácter personal, debe desarrollar el mandato constitucional establecido en el artículo 2 numeral 6 de nuestra Carta Magna, pues si bien el Habeas Data es una Garantía que protege contra las posibles amenazas o vulneraciones a los derechos de intimidad (principalmente), es necesario que haya una regulación que impida de lleno dichas acciones, que complementado con campañas de divulgación e información a los ciudadanos, puedan ayudar de manera efectiva en la defensa de sus derechos.

3. NUEVOS DESAFIOS AL DERECHO INFORMATICO EN EL NUEVO MILENIO

A. La Protección del Derecho a la Intimidad y Privacidad frente a las Nuevas Tecnologías.-

Los datos de carácter personal se definen como cualquier información concerniente a las personas. En concreto, toda información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona natural identificada o identificable.

El tratamiento de dichos datos puede manifestarse de diversas maneras, pero creemos que puede resumirse en las operaciones y procedimientos que permiten su recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación, o cesión.

Otro concepto que tenemos que tener en claro es el afectado con dicho tratamiento, y ese es la persona natural titular de los datos que sean objeto del tratamiento automatizado de cualquier naturaleza.

El inciso 6 del artículo 2 de nuestra Constitución nos señala de manera clara que, toda persona tiene derecho a que los servicios informáticos no suministren informaciones que afecten la intimidad personal y familiar.

Es este aspecto el que abordaremos en nuestro tema de conversación, en donde a raiz del desarrollo de las nuevas tecnologías se ha hecho muy común el tratamiento automatizado de datos, y por la cual se hace cada vez más necesaria una regulación específica.

El Habeas Data, si bien es una garantía constitucional que protege los derechos reconocidos en el inciso 6 del artículo 2 de la Constitución, sólo será efectiva cuando exista una vulneración o amenaza de vulneración al derecho citado. Sin embargo no existe un ente que registre todos los archivos automatizados de datos personales, y pensamos que es por aquí donde debería comenzarse a trabajar.

Tanto instituciones públicas como privadas, mantienen grandes archivos automatizados de datos de carácter personal, sin haber tenido ningún tipo de supervisión ni mucho menos de recomendación advirtiendo los límites de utilización de dichos datos. Para comenzar diremos que limitar el uso de la informática y de otras técnicas y medios de tratamiento automatizado, augurarán una mejor protección al honor, intimidad personal y familiar de los ciudadanos.

B. Principios en el Tratamiento Automatizado de Datos de Carácter Personal.-

Debemos partir reconociendo, que tipo de datos son los que se están almacenando en archivos automatizados. Por ejemplo, la doctrina española denomina a este aspecto "calidad de los datos", los cuales hacen referencia a que los datos sean adecuados, pertinentes y no excesivos en relación con el Ámbito y finalidades legítimas para las que se hayan obtenido.

Dentro de la información almacenada, existe datos de carácter muy sensible y que merecen una protección especial, como por ejemplo:

a) Los datos referentes a la ideología, religión o creencias, en donde nadie puede ser obligado a declararlos, salvo que el titular de la información lo consienta de manera expresa. Además al intentar solicitar ese tipo de informaciones debe existir la obligación de advertir al interesado su derecho a NO prestar su consentimiento si lo quiere.

b) Los datos referentes al origen racial, salud o vida sexual, los cuales tienen una connotación muy íntima en donde solo podría justificarse su solicitud por razones de interés general y cuando lo disponga una ley o cuando el titular de la información consienta expresamente.

c) Los datos protegidos por propia norma, en este caso aquellos datos relativos a la comisión de infracciones penales o administrativas, sólo podrán incluirse en archivos públicos por la Administraciones competentes de acuerdo con los previsto en sus normas reguladoras.

C. La Seguridad en el Tratamiento Automatizado de datos de Carácter Personal.-

Un aspecto muy importante en el almacenamiento automatizado de datos, es la seguridad con la que se cuente para protegerlos. Es lógico pensar, que el responsable de dicha seguridad está en la persona quien haya almacenado dicha información, sea esta una persona natural o jurídica. En ello, lo importante es evitar tanto la alteración, pérdida y determinar el acceso no autorizado de tan preciado bien como lo es la información de carácter personal, y eso sólo puede lograrse teniendo las condiciones adecuadas para garantizar la integridad y seguridad de dichos datos. Y ello, debería estar vigilado por una Entidad idónea que reglamente estas condiciones.

Por último, un punto muy importante en el almacenamiento automatizado de datos de carácter personal es el deber de secreto que debe guardar el responsable del archivo que contenga dicha información, que ade-

más debe alcanzar a aquellas personas que están involucradas en cualquier fase del tratamiento, incluso después de haber finalizado la relación con el titular de los datos o el responsable del archivo.

De otro lado, debe existir como regla general que todo tratamiento automatizado requiera el consentimiento del afectado, que como dijimos es aquella, de quien se conserve información de índole personal.

D. El Consentimiento del Afectado en el Tratamiento Automatizado de Datos de Carácter Personal.-

La intimidad es sin duda el gran protagonista en el tratamiento automatizado de datos de carácter personal, por ello es importante definirla de alguna manera. En la actualidad hay un concepto denominado "autodeterminación informativa", la cual se conoce como "el derecho a que el individuo pueda decidir sobre que aspectos desea revelar acerca de sus pensamientos, sentimientos, conductas o hechos de su vida personal". Este concepto es el que se utiliza digámoslo "modernamente" para definir ahora lo que es la intimidad.

Aunque no vamos a profundizar acerca de las bases de datos que contengan información sobre personas jurídicas, si sería necesario indicar, que también ellas pueden ser "víctimas" del tratamiento automatizado, el cual puede vulnerar derechos como el de confidencialidad y por la cual mantienen su "buena imagen" y prestigio ante los demás.

Pero volviendo al tema en cuestión, el consentimiento del que estamos hablando, es aquella mediante el cual de manera expresa e indubitable el afectado manifiesta su voluntad de que sus datos personales puedan ser tratados automatizadamente. Este derecho, que asimismo es un deber que deben cumplir los responsables de archivos de este tipo, se basa en la solicitud de autorización al afectado para poder almacenar información que le concierne, y que pueda contener datos de los denominados sensibles al pertenecer al carácter privado y/o íntimo de las personas, y por ello la necesidad que se efectúe tomando todas las precauciones que eviten posibles malos tratamientos. Sin embargo, debe indicarse que el consentimiento de voluntad sólo será válido cuando los datos NO sean recolectados de manera fraudulenta, desleal o ilícita, pues caso contrario dicho consentimiento puede ser revocado en cualquier momento. Así también, en el caso de las informaciones que merecen una protección máxima, el titular de dicha información tiene el derecho a no prestar su consentimiento.

Al solicitar el consentimiento al titular de los datos de carácter personal, será necesario que se le informe de:

- La existencia de un archivo automatizado
- De la finalidad del mismo
- De los destinatarios de la información
- Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le haga.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.
- De la identidad y dirección del responsable del archivo.

Existen también excepciones que pueden tomarse en cuenta al consentimiento del afectado y éstas pueden enumerarse de la siguiente manera:

- Que una ley disponga otra cosa
- Que la recolección de datos se haga en fuentes accesibles al público, siempre que los datos provengan de archivos de titularidad privada

- Que se recoja la información para el ejercicio de las funciones propias de las Administraciones Públicas

- Que se refieran a personas vinculadas por una relación negocial, laboral o administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato

- Que la recolección deba efectuarse obligatoriamente por mandato judicial

- En caso de necesidad pública o interés nacional

E. Derechos derivados del Tratamiento Automatizado de Datos de Carácter Personal.-

Como consecuencia del tratamiento automatizado de datos de carácter personal, los afectados pueden ejercer ciertos derechos de carácter personalísimo, y que por su naturaleza sólo pueden ser ejercidos por ellos mismos o por sus representantes legales. Estos son:

a) Derecho de impugnación.

La valoración de la conducta de una persona que sólo toma como referencia un tratamiento automatizado de datos de carácter personal, puede ser impugnada por el afectado, pues la definición o características de personalidad que puedan estar archivadas, pueden ayudar a conocer el comportamiento de la persona mas NO a determinarla.

b) Derecho de información.

En el tratamiento automatizado de datos es imprescindible que se comunique al afectado aquella información que enumeramos al tratar sobre el consentimiento, las cuales deben expresarse de modo expreso, preciso e inequívoco. Asimismo, debería existir una entidad autónoma que registre a aquellos archivos automatizados que contengan datos de carácter personal, ya que sólo así podrá ser posible el ejercicio de los derechos de acceso, rectificación y cancelación del afectado.

c) Derecho de acceso.

Es la facultad que se reconoce al titular de los datos de carácter personal que se encuentren archivadas automatizadamente, para recabar información de sus datos incluidos y tratados.

Este derecho deberá ejercerse mediante una solicitud o petición dirigida al responsable del fichero utilizando cualquier medio que permita acreditar el envío y recepción de la solicitud. Para ello, el responsable del archivo deberá resolver la solicitud en un plazo determinado contado a partir de la recepción de la solicitud. Sin embargo, pueden existir casos en donde se deniegue la solicitud interpuesta, entre ellas:

En el caso de archivos de titularidad privada.

- Cuando la solicitud sea llevada a cabo por persona distinta del afectado

En el caso de archivos de titularidad pública.

- Cuando el ejercicio del derecho de información pueda afectar o amenazar la defensa del estado, la seguridad pública o la protección de derechos y libertades de terceros.

d) Derecho de rectificación y cancelación.

Son aquellos por los cuales, el afectado puede obligar al responsable del archivo a que mantenga la

exactitud de los datos, rectificando o cancelando aquellos que resulten incompletos o inexactos, o bien sea inadecuados o excesivos en su caso. Es importante señalar que el responsable del archivo automatizado tiene la obligación de mantener la exactitud y veracidad de los datos que almacena, sin embargo puede no acceder a lo solicitado siempre y cuando lo comunique motivadamente al afectado. Aquí podemos decir entonces, que el afectado en el tratamiento automatizado de datos, está dando un primer paso para poder ejercer su derecho a información, y que éste al no ser respondida, se convierte en una vulneración a su derecho y por el cual pueda interponer la denominada Acción de Habeas Data.

F. Situaciones Especiales de Archivos Automatizados de Carácter Personal de Titularidad Pública y Privada.-

Archivos de titularidad pública :

Hemos mencionado que existen algunas excepciones en donde el responsable público de los archivos automatizados de carácter personal puede negarse a cumplir con los derechos de información, rectificación o cancelación de datos, ellas podrían resumirse de la siguiente manera:

Cuando se trate de archivos correspondientes a:

- Las fuerzas armadas o tengan fines policiales en función de los peligros que puede acasionar en defensa del estado o la seguridad pública, la protección de derechos y libertades de terceros o necesidades de investigaciones.

- La Administración Tributaria, cuando el afectado está siendo objeto de actuaciones inspectoras

- La persecución de infracciones penales o administrativas

Archivos de titularidad privada :

Igualmente, hay situaciones en que el archivo automatizado de datos de carácter personal, tiene un carácter especial en donde tanto su protección como tratamiento deben darse con mucho mayor cuidado, pues los datos que manejan deben mantener esa protección máxima que hablabamos anteriormente. Entre ellas podemos mencionar:

- Archivos mantenidos por partidos políticos, sindicatos e iglesias

- Datos sobre los abonados de servicios de telecomunicaciones

- Prestación de servicios de tratamiento automatizado de datos

- Prestación de servicios de información sobre solvencia patrimonial y de crédito

- Archivos con fines de publicidad

- Archivos relativos a encuestas o investigaciones

Hay también casos de archivos de titularidad pública que se rigen por sus disposiciones específicas o normas propias. Estos serían los casos de:

- Archivos correspondientes al Régimen Electoral

- Archivos correspondientes a registros civiles o de antecedentes penales o policiales

- Archivos correspondientes a la función estadística o investigación pública (INEI)

G. Conclusión.-

La salida al mercado de nuevas tecnologías, ha estado acompañado de nuevos formas de vulneración a los derechos de las personas, sobretodo las que se refieren a la intimidad y/o privacidad de las mismas. Al respecto cabe señalar que los datos de carácter personal deben tener una regulación específica, la cual debe indicar las formas y procedimientos adecuados al mismo.

Los procedimientos de acceso a datos personales sólo pueden darse tras el consentimiento expreso del afectado. Es decir sólo el consentimiento del afectado puede justificar un tratamiento que no viole el derecho a la intimidad y/o privacidad. El avance de la tecnología actual y el desarrollo de los medios de comunicación de masas, han obligado a que se extienda esta protección más allá de lo que pueda hacer una Acción de Garantía (caso del Habeas Data).

Por otro lado, el tratamiento automatizado de datos de alguna manera, puede conservar información sobre costumbres, inclinaciones, intereses y gustos, convirtiéndose en una mercancía que podríamos llamar "perfiles personales" y que muchos no dudarían en comprarla.

En este mismo sentido, el tratamiento automatizado de datos debe darse en un marco en donde se deba tomar las medidas adecuadas para salvaguardar la seguridad de los mismos ante todo riesgo concreto de violación. También debemos mencionar que, el tratamiento automatizado de datos personales debe basarse en ciertos principios como la calidad de datos, su recolección y almacenamiento lícito y su demostración limitada. De ello podemos desprender lo siguiente: a) que se podrá enseñar datos personales sólo a aquellos que están autorizados a verlos, b) sólo podrá permitirse la modificación de datos personales con métodos, medios y procedimientos regulados, c) que la demostración de los datos personales sólo se deberá ser revelado a personas autorizadas, y d) la existencia de un sistema de protección adecuado en el revelado de datos personales.

Estos mecanismos legales que deberían existir por su imperiosa necesidad actualmente, nos hacen reflexionar sobre el desarrollo del fenómeno informático en nuestra sociedad y que ha traído consigo una mayor vulnerabilidad de las libertades del individuo y la invasión frecuente de su esfera privada y/o íntima, situaciones que para el derecho y sobretodo para los legisladores no deben ser indiferentes. Por otro lado, la existencias de redes de información (como por ejemplo INTERNET), también sirven ahora como grandes archivos de almacenamiento de datos personales y su tratamiento también debe estar controlado, aunque en este sentido es la voluntad de cada persona el que determinará si desea que sus datos aparezcan en dicho medio, y asumir los riesgos que ello conlleva.

Si bien es cierto que, actualmente el objetivo de grandes empresas y del estado se centra en el dominio de la mayor cantidad de información que le sea posible almacenar, no deben olvidar que su derecho a estar informado y a comunicar no debe ser motivo para que en su ejercicio, vulneren otros derechos como el de intimidad y/o privacidad de terceros, sin que esto signifique en ningún caso el menoscabo del derecho de información.

Sin embargo, debemos tomar en cuenta que las grandes redes de información, nos brindan cada vez más servicios (ej: correo electrónico, bolsas de trabajo, bolsas de valores), en donde casi de manera general se solicita datos personales y por la cual muchas veces, el tratamiento automatizado de los mismos escapa a las legislaciones locales. Es por ello que sólo "la autodeterminación informativa", mencionada anteriormente será la que pueda establecer en que medida queremos que están protegidos nuestros derechos a la intimidad y/o privacidad.

Llegará un momento en donde la tan mentada globalización también tocará las puertas del derecho, sobretodo en materia informática y por el cual deberíamos a tomar conciencia de ello y sobretodo de trabajar para ello.

"La influencia de la informática en la actividad probatoria y su regulación en Uruguay"

Dra. Esc. María José Viega Rodríguez (Uruguay)
Doctora en Derecho y Ciencias Sociales. Escribana Pública

1. INTRODUCCION.

Hemos comenzado un nuevo milenio. El ejercicio de la abogacía ya está en proceso de transformación debido al avance vertiginoso de la tecnología. Y como bien dice Julio Núñez Ponce:[1] *"el rol del abogado en la sociedad virtual será cada vez más frecuente e importante, dado el constante crecimiento del comercio electrónico y de los conflictos legales que surgen en forma cada vez más frecuente en el ciberespacio."*

El objetivo de presentar esta ponencia es trasmitirles mi inquietud, ante una problemática que dejó de ser una posibilidad para convertirse en una realidad, y es el tema de la prueba informática.

La actividad probatoria no ha quedado fuera de la influencia de la informática, y en nuestro país se ha venido dando un proceso legislativo tendiente al reconocimiento de aquellos documentos que emanan de las nuevas tecnologías. En este trabajo daré un panorama de la legislación existente en Uruguay en relación al tema.

2. EL DOCUMENTO ESCRITO Y EL DOCUMENTO INFORMATICO.

Existen distintos enfoques en relación a estos dos tipos de documentos, el escrito y el informático. Están aquellos autores que entienden que los registros informáticos no constituyen un escrito y se basan en las diferencias entre uno y otro, pero también existen los que les encuentran muchas similitudes y opinan que el documento electrónico es otra forma de escribir. Sin lugar a dudas ambos tienen razón, existen diferencias, pero también existen aspectos en que ambos se parecen.

Las diferencias entre ambos podemos decir que son las siguientes:

a) Un documento escrito no puede concebirse sin el soporte material que es el papel. Sin embargo esto no siempre fue así. Existen a lo largo de la historia muchísimos tipos de documentos que nos demuestran la existencia de un hecho y que no necesariamente fueron realizados en soporte papel. Por otra parte, el papel, tan importante en nuestra civilización no lo ha sido en el pasado, y no veo razones de peso por lo que deba serlo en el futuro. Y aquí no podemos obviar el problema de la seguridad, que, para quienes escribían en las cavernas, sobre la piedra, el papel no les resultaría seguro en absoluto, al igual que como hoy algunos dudan de la seguridad de los soportes informáticos.

   Al respecto nos dice Bill Gates: "Durante más de 500 años, todo el volumen del conocimiento y de la información humanos se ha almacenado en forma de documentos de papel. (...) el papel estará siempre con nosotros, pero su importancia como medio de buscar, preservar y distribuir información está disminuyendo ya"[2].

b) Otra diferencia que se enuncia es que el registro informático puede ser fácilmente modificado, mientras que el documento escrito puede resultar más difícil de modificar sin dejar huellas en él. Creo que el gran avance de la técnica, no sólo en materia informática, desmiente esta afirmación.

---

[1] Núñez Ponce, Julio. "Ejercicio de la abogacía en Internet en la especialidad de Derecho Informático", Revista Electrónica de Derecho Informático (REDI) Número 18 enero, 2000 (consultada el 04/01/2000).

[2] Gates, Bill. "Camino al futuro", Ed. Mac Graw-Hill, España, 1996, Segunda Edición.

Las fotocopiadoras láser color, por ejemplo, permiten realizar copias de una calidad tal que nos resultaría muy difícil distinguir el original de la copia a simple vista.

c) Otro tema importante es la firma. La firma ológrafa no es la única forma de identificar a una persona, ésta también es falsificable y sólo un perito calígrafo nos dirá que grado de originalidad tiene. La firma electrónica ya es una realidad entre nosotros, así como las empresas certificadoras de las mismas. Esto ha planteado un gran desafío para los notarios, que hasta el momento eran los únicos investidos para realizar certificación de firmas. En Uruguay la autoridad certificante es la Dirección Nacional de Correos.

d) Una diferencia importante es que en el documento informático desaparece la diferencia entre la copia y el original. Esta es quizá una de las apreciaciones más valederas, porque no es posible distinguir entre un documento informático original y su copia.

Con relación a las <u>similitudes</u> podemos decir que:

a) Se considera en nuestra época a la informática como un nuevo lenguaje, hablamos de que en este siglo que se inicia, quienes no conozcan el manejo informático serán considerados analfabetos, ya que podemos considerar el lenguaje binario como un alfabeto. El nivel de educación en esta área crece a pasos agigantados. Cuando comencé la Aspirantía Docente en Informática Jurídica, hace siete años, eran muy pocos los estudiantes de abogacía que tenían conocimientos de informática y se limitaba al manejo de un procesador de texto. Comenzábamos el curso describiendo una computadora, porque no todos tenían acceso a ella. Hoy por hoy, los jóvenes han integrado la informática a sus vidas, por lo tanto a su carrera universitaria, aportan material obtenido en Internet y las bases de datos son una herramienta más en su vida jurídica. Para estos futuros colegas, el uso de la tecnología en materia de prueba será sin duda una herramienta importantísima, que todos nosotros debemos incorporar a la actividad cotidiana.

b) El lenguaje binario es criticado porque no puede ser leído directamente. La música también se escribe en forma diferente, y es leída sólo por aquellos que saben solfeo, sin embargo las partituras musicales no han planteado problemas. Tengamos presente que la ley no establece con que signos debe manifestarse la escritura.

c) El carácter de indestructibilidad del soporte no constituye una exigencia legal, también el papel se destruye, por el fuego o la humedad. Con respecto a la posibilidad de modificación del documento informático frente a lo irreversible que puede ser el documento escrito, quizá podría ser cierto cuando pensamos en los Protocolos de los escribanos realizados en tinta negra de buena calidad, pero no lo será si pensamos en un documento enviado por fax, que al ser recibido en un papel estándar de transferencia térmica tiende a ser borrado. Y la realidad nos demuestra que hoy, a nivel mundial, un alto porcentaje de contratos se realizan por fax, a través de redes privadas, por correo electrónico o a través de Internet.

3. NUESTRO DERECHO POSITIVO.

En este punto me interesa mostrar la evolución de nuestro derecho en forma cronológica y de que manera se han ido adecuando las normas a los cambios tecnológicos en materia de prueba.

3.1 Código General del Proceso del 18/10/1988.

<u>Art. 77</u>- *"La notificación se practicará ... o por el medio idóneo que habilite la Suprema Corte de Justicia".*

Tenemos la posibilidad de que la Suprema Corte reglamente por acordada el uso de medios electrónicos para realizar las notificaciones dentro del proceso judicial.

Art. 146.2. *"También podrán utilizarse otros medios probatorios no prohibidos por la regla de derecho, aplicando analógicamente las normas que disciplinan a los expresamente previstos por la ley".*

Si bien no menciona expresamente los medios electrónicos, deja una puerta abierta a su utilización.

Art. 170.2 *"Los demás documentos privados emanados de las partes, se tendrán por auténticos, salvo que se desconozca su firma, si están suscritos o la autoría, si no lo están, ...".*

Con relación a estos tres artículos el Dr. Bauzá[3] comenta: *"El caso en que todos los artículos vinculados a la "prueba por documentos" (privados), la Comisión Legislativa que estudiaba el proyecto de ley introdujo ciertos cambios llamativos en la redacción de los textos respectivos, trocando ciertas expresiones limitativas como la de "suscritos" (o "manuscritos") por la más amplia de "emanados".* Y agrega a pie de página que *"El Proyecto definitivo fue aprobado como ley, prácticamente a tapas cerradas en ambas Cámaras."*

Con estos artículos se destierra la idea restrictiva de documento, como aquel escrito y firmado por su autor. El "documento electrónico" podrá ser admitido en virtud a estas normas. Las Escribanas Siri y Wonsiak[4] llegan a la siguiente conclusión: *"Los documentos electrónicos que se sustentan en otro tipo de soporte, por la imposibilidad de cumplir con las "formas requeridas" –las que fueron pensadas para el documento papel-, en el estado actual de nuestra legislación no pueden ser documentos públicos, pero sí pueden llegar a alcanzar el valor de documento privado reconocido, si se dan las circunstancias para ello."*

Art. 177.1 *"Procede la prueba pericial, cuando para verificar hechos que interesan al proceso son necesarios conocimientos artísticos, científicos o técnicos especiales".*

Los peritos expertos en informática ya se están utilizando en nuestras sedes judiciales, en temas relacionados por ejemplo a la piratería de software, a los efectos de establecer que programas se encuentran instalados en las máquinas y acerca de su originalidad.

3.2 Ley 16.002 del 25/11/1988.

Art. 129. *"La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido".*

Art. 130. *"El que voluntariamente trasmitiere a distancias entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda".*

Estos artículos regulan la autenticidad y prueba de los documentos trasmitidos a distancia por medios electrónicos entre dependencias oficiales. Y los delitos a que alude son los que penalizan la falsificación documentaria.

3.3 Ley 16.060 del 5/1/1990.

Art. 11. *"En el Registro Público de Comercio, realizada su inscripción, se formarán un legajo para cada sociedad, con las copias del contrato social, sus modificaciones y demás documentos que disponga la ley o su reglamentación. Su consulta será pública.*

La Reglamentación podrá autorizar el empleo de todos los medios técnicos disponibles para el cumplimiento de lo dispuesto en el inciso anterior".

---

[3] Bauzá Reilly, Marcelo. "Aperturas del Derecho de la Prueba en Uruguay en materia de nuevas tecnologías de la información".

[4] Siri, Julia y Wonsiak, María "El documento electrónico". Revista de la Facultad de Derecho y Ciencias Sociales, Montevideo, 1988.

Si bien resulta muy interesante la amplitud de este artículo, al referirse a "medios técnicos" fue suspendida la vigencia por la Ley 16.170 que en su artículo 383 establece *"Suspéndese la aplicación del artículo 11 de la Ley 16.060, de 4 de setiembre de 1989, hasta que el Poder Ejecutivo proceda a su reglamentación, la cual deberá dictarse cuando a su juicio se disponga de los medios técnicos apropiados, para la formación del legajo o de información equivalente"*.

Art. 91. *"La reglamentación establecerá las normas contables adecuadas a las que habrán de ajustarse los estados contables de las sociedades comerciales.*

Asimismo podrá autorizar para estas sociedades, el empleo de todos los medios técnicos disponibles en reemplazo o complemento para estas sociedades de los libros obligatorios impuesto a los comerciantes".

3.4 - Decreto 500/91

Art. 14. *"Es de interés público, para mejor cumplimiento de los servicios, el intercambio permanente y directo de datos e información entre todas las unidades y reparticiones de la Administración Pública, sea cual fuere su naturaleza jurídica o posición institucional, a través de cualquier medio hábil de comunicación, sin más limitación que lo dispuesto en el artículo 80.*

A efectos de implementar sistemas de libre flujo de información se propenderá a la interconexión de los equipos de procesamiento electrónico de información u otros similares.

Asimismo podrá la Administración brindar el servicio de acceso electrónico a sus bases de datos a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren".

Este decreto es de suma importancia, ya que está enmarcado en el ámbito de la Reforma del Estado, en lo concerniente al proceso de desburocratización del mismo. Tengamos presenta las palabras de Bill Gates[5]: *"La administración, quizá más que ninguna otra organización saldrá ganando con la eficiencias y la mejora del servicio que derivan de los procesos digitales. Los países desarrollados van a mostrar el camino de cómo se crean procesos sin papel para reducir la burocracia. Sin embargo la mayoría de las administraciones andan muy rezagadas, en comparación con las empresas, por lo que se refiere al empleo de los instrumentos de la era digital."*

Art. 19 inciso final. *"Asimismo las dependencias de la Administración Central podrán admitir la presentación de los particulares por fax u otros medios similares de transmisión a distancia, en los casos que determinen"*.

Art. 32. *"La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación automática y hará plena fe a todos sus efectos en cuanto a la existencia del original transmitido.*

El que voluntariamente transmitiere a distancia entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda (Ley 16.002 arts. 129 y 130)".

Este artículo es de fundamental importancia en la medida que equipara este tipo de documentos al documento público, ya que establece que el mismo hará plena fe.

Art. 33. *"En aplicación a lo dispuesto por el artículo 14, la Administración propiciará el uso de soportes de información electrónicos, magnéticos, audiovisuales, etc., siempre que faciliten la gestión pública"*.

Art. 70 inc. 1. *"Los hechos relevantes para la decisión de un procedimiento podrán acreditarse por cualquier medio de prueba no prohibido por la ley"*.

---

[5] Gates, Bill. "Los negocios en la era digital". Editorial Sudamérica. 1999. pag. 403

Cualquier medio de prueba, dice este artículo, o sea que podemos utilizar tecnología actual o futura, y dependerá de nuestra imaginación el alcance que podamos darle. Sin duda, este artículo rige en el ámbito del procedimiento administrativo, pero no debemos olvidar que en el Código General del Proceso existe una norma similar que establece que podrán utilizarse otros medios probatorios no prohibidos por la regla de derecho.

Art. 90. *"Autorízase la copia fotográfica y microfilmada de los expedientes y demás documentos archivados en todas las dependencias del Estado y demás Organismos Públicos, y la destrucción de los documentos originales cuando ello sea indispensable, de conformidad con las normas reglamentarias vigentes o a dictarse.*

Dichas copias tendrán igual validez que los antecedentes originales a todos los efectos legales, siempre que fueren debidamente autenticadas por las Direcciones de las respectivas Oficinas (Ley 14.106, de 14 de marzo de 1973, art. 688)".

Evidentemente lo que se busca aquí es ganar espacio físico y mejorar la búsqueda de información. Pero la crítica que podemos hacerle a este artículo, es que se trata de una norma cerrada, ya que la misma enumera en forma taxativa los medios técnicos que pueden utilizarse, eliminando la posibilidad de aplicar nuevas tecnologías.

Art. 91 inciso final. *"También podrá practicarse la notificación a domicilio por telegrama colacionado certificado con aviso de entrega, por carta certificada con aviso de retorno, télex, fax o cualquier otro medio idóneo que proporcione certeza en cuanto a la efectiva realización de la diligencia y a su fecha, así como en cuanto a la persona a la que se ha practicado".*

Si bien establece que se puede notificar por cualquier otro medio idóneo, pone como condición fundamental al existencia de certeza en la actuación.

Art. 154 inciso primero. *"Cualquiera sea la forma documental utilizada para la interposición de los recursos (escrito en papel simple, formulario o impreso, telegrama colacionado certificado con aviso de entrega, télex, fax, o cualquier otro medio idóneo), siempre deberá constar claramente el nombre y domicilio del recurrente y su voluntad de recurrir traducida en la manifestación de cuales son los recursos que se interponen y la designación del acto administrativo que impugna".* (ver art. 19)

Art. 157. *"En caso de que los recursos se hayan interpuesto mediante telegrama colacionado certificado con aviso de entrega, télex, fax, u otro procedimiento similar, por razones de conservación de la documentación y seguridad jurídica, la Administración procederá de inmediato a su reproducción a través de los medios pertinentes y formará el correspondiente expediente. El jefe o encargado de la unidad de administración documental extenderá la correspondiente certificación de la reproducción realizada.*

En los casos señalados precedentemente, el recurrente o su representante dispondrá de un plazo de diez días hábiles a contar del siguiente a la recepción del correspondiente documento por la Administración, para comparecer en la oficina a efectos de ratificar por escrito su voluntad de recurrir, de cumplir con la exigencia legal de la firma letrada, para la agregación del mandato respectivo en caso de representación y, en general, para cumplir con todo otro requisito que para el caso sea exigible. Si no lo hiciere dentro del plazo señalado, sin justa causa, la Administración tendrá el recurso por no presentado".

El avance que establece el artículo 154 se ve disminuído por la exigencia planteada por el art. 157 al deber comparecer a ratificar, como forma de dar seguridad al acto jurídico.

Art. 158 inciso final. *"En los demás procedimientos referidos en el artículo anterior, se tendrá por fecha y hora de recepción, la que luzca el reporte emitido por el equipo utilizado o, en su defecto, la que estampa el funcionario receptor".*

Sin embargo, aquí se confía en la fecha y hora que emita el equipo utilizado. Cuando se redactó este artículo se pensaba en el fax como medio de comunicación.

Art. 195. *"Los hechos relevantes para la decisión del procedimiento disciplinario podrán acreditarse por cualquier medio lícito de prueba (fotografías, fotocopias, croquis, cintas magnetofónicas, así como por todo otro medio hábil que provea la técnica)".*

Este es un caso de artículo abierto, en el cual el software podría estar comprendido.

3.5 - Ley 16.226 del 29/10/91

Art. 383. *"El tribunal de lo Contencioso Administrativo podrá, en forma directa o por concesión de terceros, brindar el servicio de acceso electrónico digital a sus bases de datos de jurisprudencia y gestión, por medio de la red telefónica pública, a las personas físicas o jurídicas, estatales, paraestatales o privadas que así lo solicitaren. El Tribunal de lo Contencioso Administrativo fijará los precios de los servicios, que no podrán superar los precios del mercado".*

Art. 384. *"Las comunicaciones procesales a las partes podrán efectuarse también por medios electrónicos o de similares características. Los documentos emergentes de la transmisión, constituirán documentación auténtica que hará plena fé a todos sus efectos, siendo de aplicación lo dispuesto por el artículo 130 de la Ley Nº 16.002 del 25 de noviembre de l988.*

El Tribunal de lo Contencioso Administrativo determinará y reglamentará la forma en que se practicarán las mismas".

3.6 Ley 16736 del 5/1/1996

Art. 694. *"Las administraciones públicas impulsarán el empleo y aplicación de medios informáticos y telemáticos para el desarrollo de sus actividades y el ejercicio de sus competencias, garantizando a los administradores el pleno acceso a las informaciones de su interés".*

Consagra "el derecho de acceso" por parte del administrado sobre informaciones de su interés y se lo ha considerado también como el germen del llamado "derecho de rectificación". El Dr. Delpiazzo[6] sostiene con razón que ya está consagrado en el art. 14 del Pacto de San José de Costa Rica, el cual fue ratificado por ley en nuestro país y que dice: *"toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio... y que se dirijan al público en general tiene derecho a efectuar su rectificación o respuesta"..*

Art. 695. *"Los trámites y actuaciones que conforman el procedimiento administrativo así como los actos administrativos podrán realizarse por medios informáticos.*

Su validez jurídica y valor probatorio serán idénticos a los de las actuaciones administrativas que se tramiten por medios convencionales.

La firma autógrafa podrá ser sustituída por contraseñas o signos informáticos adecuados".

Equipara los medios informáticos a los convencionales, reconoce su validez jurídica y les otorga el mismo valor probatorio. El inciso final de este artículo está consagrando la firma electrónica digital.

Art. 696. *"La notificación personal de los trámites y actos administrativos podrá realizarse válidamente por correo electrónico u otros medios informáticos o telemáticos, los cuales tendrán plena validez a todos los efectos siempre que proporcionen seguridad en cuanto a la efectiva realización de la diligencia y a su fecha".*

---

6 Delpiazzo, Carlos E. "Derecho Informático Uruguayo". Montevideo 1995, pag. 60.

Hablar de notificaciones por correo electrónico es sin duda un gran avance, en cuanto a la rapidez con que se pueden realizar las actuaciones. Sin embargo, el legislador nunca pierde de vista la seguridad que debe darse a estos procedimientos.

Art. 697. *"La documentación emergente de la transmisión por medios informáticos o telemáticos constituirá de por sí documentación auténtica y hará plena fe, a todos sus efectos, en cuanto a la existencia del origen trasmitido".*

Vemos que esta norma amplía el artículo 129 de la ley 16.002 en dos aspectos: sustituye el término "medios electrónicos" por "medios informáticos y telemáticos" y elimina la frase "entre dependencias oficiales", lo que convierte a la norma en aplicable para la generalidad.

El inciso segundo establece: *"El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda".*

Comparando con el art. 130 de la ley 16.002 podemos observar que en primer lugar hay una ampliación de los comportamientos reprimibles, en segundo lugar se elimina también aquí la expresión *"entre dependencias oficiales"* y se tiene en cuenta para quien adultere o destruya el *"documento almacenado en soporte magnético o su respaldo".*

Art. 698. *"El Poder Ejecutivo reglamentará las disposiciones contenidas en los artículos precedentes, las que no podrán implicar costos presupuestales".*

3.7 Decreto 65/998.

Y este decreto cumplió con lo prescripto por el art. 698 de la Ley 16.736 y reglamentó el procedimiento administrativo electrónico.

Art. 1. *"La sustanciación de actuaciones en la Administración Pública, así como los actos administrativos que se dicten en las mismas, podrán realizarse por medios informáticos".*

Y en el inciso segundo establece *"...constituirán instrumentos públicos y como tales se tendrán como auténticos y harán plena fe ..."*

Art. 3 inc. 1. *"El expediente electrónico tendrá la misma validez jurídica y probatoria que el expediente tradicional".*

Art. 18 y 19. Establecen la firma electrónica y digital, de suma importancia a los efectos de dar validez a la documentación electrónica.

Art. 25. Reproduce el inc. 2 del art. 697 de la Ley 16.736.

Art. 26. Reproduce el art. 130 de la ley 16.002.

4. CONCLUSIONES.

Se habla permanentemente de la inadaptación del derecho existente a las nuevas tecnologías. Y es así en algunos aspectos, pero no en todos. Michael Vivant[7] nos plantea: *Estas tecnologías que nos interesan son nuevas sin duda. Pero sobre todo crean perspectivas nuevas, obligan a ver diferentemente aquello que habíamos tomado el hábito de ver de una cierta manera y en consecuencia a dejar el dominio, confortable y un poco*

7 Vivant, Michael. "El derecho de las nuevas Tecnologías: un revelador". Revista de la Alta Tecnología. Setiembre 1998. Nº 121, Año XI.

ronroneante, de las ideas recibidas para acceder al enfoque crítico (a la crítica en el verdadero sentido del término, el sentido filosófico, sin que la palabra tenga de manera alguna una connotación negativa): pensar la regla, pensar la noción ... y no recibirla pacíficamente".

Sin duda, este es el trabajo que ha realizado nuestro gobierno, concretamente la Administración Central, que ha venido haciendo un enorme esfuerzo en post no solo de la desburocratización del Estado, como lo veíamos con el Dec. 500/91, sino también de la modernización del mismo, de la adaptación y el aprovechamiento de las nuevas tecnologías. En fin, pretendiendo estar acorde no solo al nivel de las empresas privadas, como decía Bill Gates, sino de mirar al futuro con desafío.

Vemos entonces que se han planteado grandes cambios en la Administración Central con relación al tema de la prueba, en lo que se refiere a la existencia del expediente electrónico y por ende la admisión de los documentos electrónicos (prueba electrónica); también existen normas para el Tribunal de lo Contencioso Administrativo, y llegarán sin lugar a dudas a ampliarse las ya existentes al Poder Judicial. Las puertas están abiertas y el trabajo es de todos.

BIBLIOGRAFIA

1. Correa. "Derecho informático". Depalma1987.

2. Bauzá Reylly, Marcelo; González Aguilar, Audilio; Carrascosa López, Valentín. "El derecho de la prueba y la informática". Revista de Informática y Derecho 2.

3. Correa Freitas, Ruben. "Principios del Procedimiento administrativo electrónico. Decreto del Poder Ejecutivo Nº 65/998 de 10/III/98.". Libro de Ponencias del VI Congreso Iberoamericano de Derecho e Informática. Montevideo 1998.

4. Delpiazzo, Carlos E.. "Informatización del procedimiento administrativo común". Libro de Ponencias del VI Congreso Iberoamericano de Derecho e Informática. Montevideo 1998.

5. Bauzá Reilly, Marcelo. "El derecho procesal y las nuevas tecnologías reproductoras de información". La Justicia uruguaya Tomo XCVI.

6. Bauzá Reilly, Marcelo. "El expediente administrativo electrónico" Revista de Derecho Público.

7. Siri, Julia y Wonsiak, María. "El documento electrónico". Revista de la Facultad de Derecho y Ciencias Sociales.

8. Correa Freitas, Ruben. Compilador. "Procedimiento administrativo electrónico". Oficina Nacional del Servicio Civil. Presidencia de la República. Marzo 1998.

9. Núñez Ponce, Julio. "Derecho Informático". Marsol perú Editores S.A.

10. Téllez Valdez, Julio. "Derecho Informático".

11. "Reforma del Estado. El nuevo procedimiento administrativo". Secretaría de la Presidencia de la República. Segunda edición.

12. Núñez Ponce, Julio. "Ejercicio de la abogacía en Internet en la especialidad de Derecho Informático", Revista Electrónica de Derecho Informático (REDI) Número 18 enero, 2000 (consultada el 04/01/2000).

13. Gates, Bill. "Camino al futuro. , Ed. Mac Graw-Hill, España, 1996, Segunda Edición.

14. Delpiazzo, Carlos E. "Derecho Informático Uruguayo". Montevideo 1995, pag. 60.

15. Gates, Bill. "Los negocios en la era digital". Editorial Sudamérica. 1999. pag. 403

16. Vivant, Michael. "El derecho de las nuevas Tecnologías: un revelador". Revista de la Alta Tecnología. Setiembre 1998. Nº 121, Año XI.

RESUMEN:

La motivación para presentar esta ponencia fue trasmitirles mi inquietud, ante una problemática que dejó de ser una posibilidad para convertirse en una realidad, y es el tema de la prueba informática.

Realizo como punto de partida un análisis del documento escrito y el documento informático.

Y posteriormente desarrollo en forma cronológica el proceso normativo tendiente al reconocimiento de aquellos documentos que emanan de las nuevas tecnologías, dando un panorama de la legislación existente en Uruguay, con la transcripción de los principales artículos de las leyes y decretos que regulan el tema.

Nombre: Dra. Esc. María José Viega Rodríguez
Nacionalidad: Uruguaya
Dirección: Calle 25 de Mayo 477 Esc. 46 Montevideo Uruguay.
Teléfono: 915 41 90 – 099 19 34 78
Fax: 915 41 90
Email: mjviega@adinet.com.uy

Curriculum:

- Doctora en Derecho y Ciencias Sociales.
- Escribana Pública.
- Integrante de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay.
- Aspirante a la materia Informática Jurídica en la Universidad de la República.

"E-Commerce y Derecho. Una visión sistemática"

Renato Javier Jijena Leiva (Chile)
Abogado
Profesor de Derecho Informático UGM
Diplomado en Derecho Informático - Universidad de Zaragoza / Chile
renatojijena@entelchile.net
rjijena@ucv.cl

1. INTRODUCCION (GENERALIDADES).

Una cuestión de fondo. El derecho es "respuesta", y frente a las nuevas realidades del mundo digital o telemático -ajenas al mundo de la cultura del papel- necesariamente debe evolucionar y adaptarse.

"El e-commerce es como el amor entre los jóvenes": porque todos lo hacen; muchos no saben cómo hacerlo; y siempre es más lo que se dice que lo que efectivamente se hace. Que la cita no induzca a errores. No quiero empezar con un prisma negativo. Todo lo contrario. Me considero y me declaro un "hincha" del comercio electrónico, pero hay que ser realistas y dejar de lado los mitos existentes.

Desde la óptica jurídica del e-commerce también existen mitos.

Quizás el más generalizado se refiere a que todo debe ser regulado por una norma legal expresa y a que el creciente comercio digital que se está realizando no está amparado legalmente. Quienes así piensan olvidan que las partes contratantes pueden establecer reglas específicas y someter la solución de controversias a mecanismos de arbitraje; que en temas como la aplicación de impuestos o aranceles a las transacciones on line la tendencia -a instancias de la OMC- es llegar a una total desregulación; que en cuanto al resguardo del "copyright" de las mercancías digitales se está validando legalmente el uso de mecanismos técnicos de resguardo como la encriptación; y que el uso y administración de los nombres de dominio se ha normado mediante "instancias de autoregulación" gracias a entidades como la ICANN.

Desde ya consignemos una idea o propuesta importante: en nuestra opinión, no todos los aspectos jurídicos del e-commerce deberían ser objeto de regulación legal mediante la promulgación de nuevas normas positivas.

Una idea nuestra al parecer es relevante, ya que ha sido copiada por algunos colegas sin la debida cita. El desafío jurídico es doble, y pasa por armonizar dos intereses concurrentes, ...permitir el uso amplio y eficaz de las nuevas tecnologías y ...proteger adecuadamente la confianza de los usuarios (empresarios y consumidores) en la autenticidad y seguridad de los documentos transmitidos y de los pagos realizados vía Internet.

Tratándose de hacer e-commerce mediante Internet, hay que tener presente que la red se caracteriza por la imposibilidad de ser normada localmente, conforme al ordenamiento jurídico de un Estado determinado. No respeta límites geográficos y no reconoce fronteras territoriales. Ella es "aterritorial" y constituye una realidad que -teóricamente y de aunarse los criterios necesarios (por ejemplo en cuanto a prohibir el comercio de pornografía o de contenidos ilícitos)- sólo podría llegar a regularse mediante Tratados Internacionales acordados por diversos Estados.

Personalmente he escrito bastante sobre la no regulación de Internet, a propósito de los contenidos ilícitos y de la censura a la libertad de expresión...

www.acui.cl
www.jurisweb.com/boletin/boletin20

Además del rol preponderante de la autorregulación y los mecanismos técnicos de resguardo, y aceptando que al derecho le corresponde principalmente un rol de segundo orden limitado a instar porque se adopten Tratados Internacionales, la formulación de nuevas normas legales destinadas a producir efectos en el ciberespacio deberá hacerse sin la rigidez que caracteriza a las normas jurídicas tradicionales.

Veamos en concreto o frente a temas determinados, cómo resolver el desafío jurídico planteado...

2. TOPICOS JURIDICOS FUNDAMENTALES DEL E-COMMERCE.

Nuevamente, téngase presente una idea esencial (sobre todo para el mundo jurídico): el mundo del E-C o forman hechos o realidades que ocurren en el mundo de lo digital, lo intangible e inmaterial, donde cada mensaje... -v.gr. una oferta de venta, una orden de compra enviada a un proveedor, una orden de pago a un banco, una declaración de importación de mercancías presentada a la Aduana- ... donde cada mensaje ya no está soportado en papel.

El nuevo orden social que viene acompañado con el uso de las NTI está ocasionando una serie de cambios jurídicos, los que en materia de e-commerce y en aras de lograr seguridad y certidumbre jurídica en las transacciones digitales se relacionan con los siguientes temas[1].

2.1 El problema de la formación del consentimiento.

Frente a la necesidad de determinar tanto "el momento" como "el lugar" donde se forma el acuerdo de voluntades, el problema es que *en una operación de C.E. a través de las fronteras o desde diversos países los intervinientes pueden encontrarse regidos por leyes que optan por soluciones distintas...*

Se trata de contratos "telemáticos" celebrados a distancia y entre ausentes, por ende pueden aplicarse diversas teorías o soluciones legales (de la aceptación, de la remisión o expedición, de la recepción efectiva del mensaje, etcétera). Chile soluciona el tema señalando que el consentimiento se forma cuando el destinatario o receptor de la oferta o mensaje la acepta sin modificaciones, independientemente de que el oferente o emisor se entere o no de tal aceptación (...en términos tecnológicos, cuando un mensaje haya sido recepcionado por el sistema informático del receptor).

El tema también es importante, porque tratándose de operaciones internacionales de comercio electrónico, eventualmente, en caso de desacuerdo, habrá que determinar conforme a qué legislación se resolverán y cuál será el tribunal competente para conocer de los conflictos que se susciten entre compradores y vendedores -las partes contratantes-.

2.2 La protección de la privacidad en el ciberespacio.

Concretamente se trata de la necesidad de proteger la privacidad de las personas contratantes cuyos datos circulan en las redes, los que pueden ser recopilados, procesados, almacenados y cruzados sin autorización de su titular, para posteriormente ser comercializados para realizar "marketing directo".

Esto no es fantasía. En EE. UU. ya se sanciono al ISP o proveedor de conectividad "American On Line" y a la librería "Amazón" por vender sus bases de datos con el comportamiento comercial y las preferencias de miles de norteamericanos. ¿Y si alguien no quiere que se sepa que le interesan los libros sobre nazismo, magia negra, pornografía u homesexualismo?; ¿cómo "el derecho", la norma legal, le asegura la privacidad de estos antecedentes?.

---

[1] En otras dos ponencias presentadas al Congreso se profundiza acerca de tres de estos temas, a saber, la protección de la privacidad, la asignación y administración de los nombres de dominio y la regulación de las firmas digitales y las entidades certificadoras en Chile.

Me detengo en este punto porque lo considero de la mayor importancia. El abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la intimidad, porque cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados. Esta imagen inmaterial del titular de los datos debe ser resguardada porque puede ser creada errada o dolosamente, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio.

Un dato es personal o nominativo cuando permite identificar cualquiera característica de una persona para relacionarse en sociedad, por ejemplo al consignarse en una guía de teléfonos datos generales, o cuando son de mayor importancia o sensibilidad como ocurre con la filiación política, el credo religioso que se profesa, los antecedentes laborales, la situación de salud, la mayor o menor riqueza, las operaciones comerciales que se realizan, las acciones en empresas que se poseen, los depósitos en cuenta corriente o a plazo, los impuestos pagados, etc.

El problema de fondo se origina por un conflicto entre dos intereses relevantes. Por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc. Por el otro, un interés –también muy legítimo- que poseen los gobiernos y los particulares para acceder a cierta información: ...los Estados para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quienes tienen SIDA al momento de fijar políticas de salud; y los particulares, generalmente constituidos en empresas de servicios o entidades gremiales, que para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial.

Se trata, por ende, de lograr un equilibrio y establecer límites. La interrogante a dilucidar o la hipótesis de trabajo, en consecuencia, puede ser la siguiente: ¿cómo conciliar el Derecho a la Información con el Derecho a la Intimidad?; ¿cómo equilibrar por un lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad?. Se trata de una cuestión importante por cierto, no de meras disquisiciones teóricas o doctrinarias, porque si bien es cierto el orden público social y económico de una Nación requiere que tanto el Estado como los particulares manejen determinados datos personales, sea para fijar políticas de salud o para evitar la morosidad comercial, esto no puede traducirse, al extremo, en abusos contra las personas.

Se produce -doctrinaria y legalmente- la conciliación entre el Derecho a la Intimidad y el Derecho a la Información a través del control que para el titular de los datos posibilita el denominado "Derecho de Acceso" o "Habeas Data", una nueva garantía fundamental (o un nuevo mecanismo de resguardo y tutela) que contemplan en el Derecho Comparado tanto algunas Cartas Fundamentales como las llamadas Leyes de Protección de Datos, y una consagración del "Principio de la Autodeterminación Informativa". El "Habeas Data" es una acción cautelar de rango constitucional, heredera de otro recurso y tan importante como el "Habeas Corpus", que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales -al decir de una sentencia histórica del Tribunal Constitucional alemán- "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente.

2.3 El problema de la identificación digital de las partes contratantes. Firmas digitales y Entidades Certificadoras.

Al derecho le compete lograr el reconocimiento legal de los mecanismos de identificación y encriptación de las transacciones, en aras de resguardar la seguridad e integridad de las operaciones de comercio y la autentificación de los contratantes. Es el tema del valor legal de las llamadas "firmas electrónicas o digitales".

La tradicional firma manuscrita u ológrafa se reemplaza por una llave o clave digital o magnética, mucho más segura, que permite identificar o acreditar la identidad tanto del emisor como del receptor de un mensaje así como la integridad del contenido de los mensajes intercambiados.

Para una mayor seguridad, jurídicamente se crearon las llamadas "Autoridades" o "Entidades" Certificadoras, proveedores de servicios de certificación que otorgando "Fé Pública" en el mundo del e-commerce aseguran la fiabilidad y confidencialiad de las transacciones digitales..

Podrá ser (según la respectiva opción de política legislativa) Entidad Certificadora un órgano estatal, una empresa comercial del campo de las telecomunicaciones, una red de valor agregado o VAN (así ocurre en Chile desde hace años), un banco respecto de sus clientes, *....pero una cuestión más compleja es la iniciativa de asignar la facultad de otorgar fe pública en materia de comercio electrónico exclusivamente a los tradicionales notarios o escribanos.*

2.4 El necesario valor probatorio o la admisibilidad en juicio de los documentos electrónicos.

Nos referimos a la forma de probar en un proceso los términos en que efectivamente se acordó y realizó una operación de comercio electrónico, esto es, el valor probatorio o la admisibilidad en juicio del documento electrónico, magnético o digital.

Todos los mensajes mediante los cuales se acuerda una operación de E.C. deben tener valor probatorio como tales, "per se", aunque no estén soportados en papeles sino que magnética o digitalmente.

El conflicto precisamente surge atendido que los registros donde constan las transacciones y las firmas son digitales o magnéticos y no soportados en papel, con lo cual, y ante la recurrente falta de interpretación jurídica, aún se cree que no satisfacen los requisitos legales de escrituración y firma.

Tratándose de sistemas jurídico-procesales –como el de Chile- donde rige el principio de la valoración legal de los medios de prueba y por ende sólo son tales aquellos que la ley establece y donde la prueba documental o instrumental se restringe a los soportados en papel, ...la solución más conveniente es instar por consagrar legalmente la "homologación total" entre éstos y los soportados digital o megnéticamente.

2.5 Propiedad Intelectual y Comercio Electrónico.

El tema de la protección de los derechos intelectuales en las redes digitales es de reciente desarrollo y por ende no existen criterios uniformes de tutela. En ellas circula información de distinto contenido o naturaleza, y se trata de datos, documentos, sonidos o imágenes que pueden ser de dominio público o que, soportados tradicionalmente y a nivel local -de un Estado-, están amparados por las instituciones del derecho de autor o "copyright".

El régimen tradicional autoral está siendo superado, porque históricamente fue concebido para obras soportadas material y no digital o magnéticamente. Las redes telemáticas han "desmaterializado" las obras, ya que las creaciones originales digitalizadas no se encarnan en un soporte físico concreto o en alguna de las formas envasadas que históricamente han contenido las obras artísticas e intelectuales, ...haciéndose fácil que sean ilícitamente reproducidas, transformadas y copiadas con fines comerciales o "pirateadas".

En la práctica, y en consideración a lo que hemos denominado la "aterritorialidad" de Internet, quien pone a disposición de la comunidad del ciberespacio una creación intelectual tiene además que entender que está renunciando a que se le pida autorización por el uso privado de su obra. Dicho de otra forma, debe aceptar que su derecho "patrimonial" de autor en alguna medida será menoscabado, ...salvo que adopte resguardos no jurídicos.

2.6 Dominios y Marcas en Internet.

Se trata de que toda entidad, empresa o persona natural que quiera mantener una página WEB u ofrecer sus productos en Internet estará interesada en tener debidamente inscrita su dirección virtual o dominio, en

definitiva para contar con el resguardo de su "identidad comercial", máxime cuando tienen un valor económico de mercado y pueden constituir una "marca" susceptible de aprovechamiento comercial.

Dicho de otra forma, la existencia de un sistema de registro y administración de dominios o nombres generalizados, geográficamente independientes y defendibles en todo el mundo... debe permitir identificar las direcciones virtuales (técnicamente URL).

Todo particular, empresa u órgano público puede presentar ante el ente coordinador una solicitud de registro, en orden a constituirse en asignatario o "propietario virtual" de "nombres de dominio" en Internet. Dichos nombres individualizan a entidades públicas y privadas, a Órganos del Estado y a entidades financieras, a personas jurídicas y a personas naturales, muchos de los cuales tienen debida y desde hace bastante tiempo previamente registradas las marcas comerciales respectivas.

El tema de la atribución o asignación de los nombres de dominio en Internet ha dado pie a la existencia de un fuerte grado de autoregulación. Las reglamentaciones que ha elaborado primero la IANA (Internet Assigned Numbers Authority) y después la ICANN (Internet Corporation Assigned Names and Numbers) en orden a coordinar y mantener un "Registro de Nombres de Dominio" han sido acogidas localmente o a nivel de Estados, más los órganos que la representan en cada país sólo actúan como entes coordinadores.

Comercio Electrónico, Estado y Derecho

Renato Javier Jijena Leiva (Chile)
Abogado
Profesor de Derecho Informático UGM
Diplomado en Derecho Informático - Universidad de Zaragoza
Asesor legal EAN*Chile

renatojijena@entelchile.net
rjijena@ucv.cl

COMERCIO ELECTRONICO.

Cuando pensamos en comercio o en negocios electrónicos estamos frente a un nuevo mundo social, económico y también jurídico, que se materializa mediante redes abiertas o cerradas, entre empresas o entre empresas y consumidores, al interior de un país o desde diversos Estados. Que duda cabe que el e-commerce está rodeado de demasiados mitos y que "es como el amor entre los jóvenes", ...porque todos lo hacen; porque muchos no saben cómo hacerlo; y porque siempre es más lo que se dice que lo que efectivamente se hace.

Para desmitificar y clarificar sirven las definiciones. Se ha definido el Comercio Electrónico como el intercambio telemático de información entre empresas (*business to business*) o entre empresas y consumidores (*business to consumer*) que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles (datos, documentos, imágenes, música, videos, servicios, etc.) o en un pedido electrónico de bienes tangibles. Ampliamente, se ha dicho que es el conjunto de actividades con finalidad mercantil que se realizan mediante sistemas y redes computacionales, sin que exista contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda, y que cubre no solamente actos comerciales directos sino también acciones preparatorias como las de publicidad o mercadeo.

A la base de lo que se entiende por Comercio Electrónico propiamente tal se encuentran la transferencia telemática de datos y de documentos estandarizados. Con el concepto EDI se alude precisamente al intercambio electrónico entre sistemas computacionales de información estructurada, es decir, de datos y documentos mediante formatos o estándares acordados previamente por los usuarios (generalmente grandes empresas). A efectos explicativos, puede sostenerse que el EDI es un correo electrónico o *e-mail* pero con protocolos comunes.

Este EDI puede hacerse mediante redes cerradas como son las *VAN, Value Added Network* o Redes de Valor Agregado o mediante redes abiertas como Internet, y se ha implementado para, por ejemplo, enviar una orden de compra a un proveedor, una orden de pago a un banco, una factura o una guía de despacho entre comerciantes, una planilla de declaración y pago de cotizaciones de AFP o ISAPRE, una declaración aduanera de importación de mercancías, un manifiesto de carga, etcétera.

En Chile la tramitación electrónica de las declaraciones aduaneras de importación de mercancías (el mensaje "CUSDEC"), de las órdenes de compra entre las empresas y sus proveedores, la eventual emisión de facturas digitales (hoy autorizada) y de las planillas electrónicas para la cotización y pago en materia de AFP e ISAPRES, pasa por o se ha logrado con la existencia de empresas que prestan servicios de Redes de Valor Agregado y administran redes cerradas -como TRANSBANK –fusionada con la ex EDIBANK-, EASYMAIL, TRANSAXION y EDITRADE-, las que, utilizando "UN/EDIFACT" o el estándar de las Naciones Unidas para el intercambio electrónico de datos o documentos en la administración, el comercio y el transporte, realizan labores de mensajería digital o de intermediación electrónica y, muy especialmente, generan y certifican el uso de un sistema de criptografía asíncrona o asimétrico de llaves digitales

MODERNIZACION DEL ESTADO.

El Gobierno de Chile no se ha quedado atrás. El proceso de modernización de la gestión del Estado, actualmente en marcha, entre sus objetivos persigue lograr la mayor transparencia y eficiencia en la gestión de la Administración, como una condición indispensable en la modernización de los procesos de ejecución. Este proceso pasa, indefectiblemente, por la necesaria incorporación y aprovechamiento de nuevas tecnologías para el logro de los objetivos programados, particularmente en materia de gestión de adquisiciones y contrataciones.

Bajo la guía del Comité Interministerial de Modernización y de los trabajos de dos Comisiones Presidenciales asesoras, se han generalizado las iniciativas modernizadoras en base a las nuevas tecnologías, esfuerzos que de forma aislada sólo habían fructificado en materia de implementación de sistemas EDI y de Modernización del Sistema Aduanero -mediante la colaboración estrecha entre el gremio de los agentes de aduana y el Servicio Nacional de Aduanas- y al interior del Servicio de Impuestos Internos.

El primer paso se dió sólo al interior de la Administración Estatal. El pasado 26 de Junio DE 1999 se publicó en el Diario Oficial una iniciativa legal importante, que sin lugar a dudas constituye un aporte y un paso adelante para la modernización de la gestión del Estado chileno. El Decreto aludido obedece a uno de los compromisos adoptados por una Comisión Presidencial de Nuevas Tecnologías que sesionó durante 1998, en orden a dotar a los órganos estatales del marco legal que permita el uso de la informática y de las telecomunicaciones en reemplazo de sus procedimientos manuales, específicamente en lo relacionado con el uso de firmas y de documentos digitales o electrónicos, pero sólo al interior de la Administración del Estado y no en las relaciones con los administrados.

"WWW.COMPRASCHILE.CL"

Quizás el aporte más relevante de los trabajos del gobierno se relaciona con el desarrollo de un sitio WEB de información y de intermediación en materia de compras estatales. Su fundamento primario emana de lo señalado en el Programa de Reforma al Sistema de Compras y Contrataciones del Sector Público, aprobado por el Comité Interministerial de Modernización de la Gestión Pública en enero de 1998.

La operatoria del nuevo sistema pasa por la existencia de dos sub-sistemas: el de "información electrónica sobre compras y contrataciones públicas (SICCP)" -v.gr. avisos de licitaciones, divulgación de antecedentes a los proveedores, etcétera, sistema que se ha puesto en marcha, al que puede accederse en el sitio www.compraschile.cl y que próximamente será validado mediante un Decreto Supremo- y el de "intermediación electrónica", que, para efectiva y válidamente realizar contratos mediante Internet y con los particulares o empresas proveedoras requiere de un marco legal específico. Respecto del sistema de información, el Decreto encomendará al Ministro de Hacienda las labores de coordinación en materia de compras y contrataciones necesarias para las diversos Ministerios y Servicios dependientes o relacionados con ellos, para lo cual contará con la colaboración del Ministro Secretario General de la Presidencia.

REGULACION LEGAL DEL SISTEMA DE INFORMACION E INTERMEDIACION ESTATAL.

El Ejecutivo presentará a la Cámara de Diputados un proyecto de ley de bases sobre contratos administrativos de suministro y prestación de servicios. Se trata de temas que, como dicen los fundamentos de la iniciativa, vinculan a la Administración con los particulares, específicamente con empresas y mediante diversas modalidades contractuales. Entre estas destacan dos especies de contratos públicos: el "de suministro" y el "de prestación de servicios". El mensaje -el proyecto- que apunta a organizar un nuevo sistema, más simple y moderno, de adquisiciones públicas, se enmarca precisamente en un ámbito más amplio, a saber, el de la reforma de la gestión y del aparato estatal, y sus fines esenciales son lograr que en materia de adquisiciones públicas exista uso eficiente de los recursos, compras de mejor calidad, ahorros presupuestarios y mayor transparencia y probidad en los actos del Estado.

De partida define como ámbito de aplicación del proyecto (Capítulo I) a los contratos que celebre la Administración del Estado para el suministro de bienes muebles y la prestación de los servicios necesarios para apoyar el desarrollo de sus funciones. El Proyecto puede dividirse en dos grandes áreas. La primera, que se refiere a las reglas generales de los contratos administrativos y que se diferencian de las reglas generales que el Código Civil aplica a los contratos civiles (Capítulos II a V, VIII y parte de los artículos finales y transitorios). El fundamento de estas reglas especiales, es la singular naturaleza del Estado en cuanto contratante, considerando que la finalidad de sus actuaciones es promover el bien común. La segunda parte tiene que ver con la regulación del nuevo **Sistema Electrónico de Información e Intermediación de Compras y Contrataciones del Sector Público**, que incluye, entre otros aspectos, la creación de una **Dirección de Compras y Contrataciones** (Capítulos VI, VII y parte de los artículos finales y transitorios).

FIRMAS Y DOCUMENTOS DIGITALES O ELECTRONICOS.

Frente a este tema el Gobierno chileno se ha jugado a dos opciones, ambas plenamente válidas. Por un lado el debate legislativo de una Moción Parlamentaria sobre firmas y documentos digitales o electrónicos que actualmente se debate en el Senado. No obstante, y en el evento que el Parlamento chileno no sea capaz de avanzar con premura y sin mitos en estas regulaciones, el mensaje comentado más arriba faculta al Presidente de la República para dictar un Decreto con Fuerza de Ley que regule la infraestructura de firma electrónica en nuestro país.

Por cierto que en cuanto a la óptica jurídica del comercio electrónico también existen mitos. Quizás el más generalizado se refiere a que todo debe ser regulado por una norma legal expresa y a que el creciente comercio digital que se está realizando no está amparado legalmente. Quienes así piensan olvidan que las partes contratantes pueden establecer reglas específicas y someter la solución de controversias a mecanismos de arbitraje; que en temas como la aplicación de impuestos a las transacciones on line la tendencia -a instancias de la OMC- es llegar a una total desregulación; que en cuanto al resguardo del copyright de las mercancías digitales se está validando legalmente el uso de mecanismos técnicos de resguardo como la encriptación; y que el uso y administración de los nombres de dominio se ha normado mediante instancias de autoregulación gracias a entidades como la ICANN.

Se constata, lamentablemente, que hasta la fecha los esfuerzos del Comité Interministerial de Modernización no han sido acompañados por el trabajo parlamentario. En relación a un tema vital para el e-commerce como es el uso de firmas, certificados y documentos digitales o electrónicos válidos, por cierto, una materia que necesariamente debe ser regulada por ley porque involucra aspectos de orden público jurídico y económico, más que mitos existe un enorme y grave desconocimiento. Hace poco un senador, durante un seminario sobre nuevas tecnologías organizado por el Ministerio de Economía, demostró un enorme desconocimiento cuando afirmó que la discusión para aprobar el uso de firmas electrónicas en Chile sería larga y compleja y que pasaría por revisar el rol de los notarios como depositarios de la fe pública, mismo que eventualmente -según el parlamentario- se vería menoscabado. Olvida el parlamentario que desde 1995 en Chile operan Redes VAN que certifican el uso de firmas electrónicas sin que participen los notarios; que tratándose de operaciones de comercio exterior electrónico realizadas en Internet ningún rol pueden jugar funcionarios públicos limitados por su competencia territorial y local; y, por último, que plantear en este contexto la ingerencia de los notarios y no de entidades certificadoras especializadas implica encarecer los costos y dilatar el tiempo de realización de las transacciones virtuales, lo que en última instancia afectará al desarrollo de la economía del país.

Por nuestra parte y atendido lo solicitado por el Presidente de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado de la República, mediante un informe evacuamos nuestra opinión académica y jurídica en relación al *Boletín Nº2348-07* que contiene una moción por la cual se inicia un *"Proyecto de Ley sobre Documentos Electrónicos"*. El documento puede bajarse integramente del site www.modernización.cl (véase "sitios relacionados").

Por tratarse de temas nuevos que desafían a las instituciones tradicionales del derecho; atendidas las necesarias mejoras de forma y de fondo a incorporar en la moción; y por referirse la materia a temas de gran rele-

vancia para el Comercio Electrónico tanto nacional como internacional de Chile y para el ordenamiento jurídico tradicional, a saber, a la firma y a los documentos digitales o electrónicos y al valor probatorio de los mismos, el informe parte por consignar algunos conceptos esenciales en materia de Comercio Electrónico vía redes, cerradas o abiertas, y rescata las iniciativas más importantes que en este ámbito actualmente y desde hace varios años se están desarrollando en Chile. Se exponen luego los aspectos jurídicos involucrados en el Comercio Electrónico (es una necesaria visión de contexto), sobre todo cuando se realiza mediante redes abiertas como Internet, para detenerse principalmente en los temas de la necesidad de resguardar la "Fe Pública" involucrada en el uso de las llamadas "Firmas Digitales o Electrónicas" y su necesaria "Certificación" tecnológica y jurídica a cargo de "Proveedores de Servicios de Certificación, y en el problema del valor probatorio de las firmas y los documentos digitales o electrónicos o de cómo acreditar legalmente en un proceso los hechos de que ellos dan cuenta. Luego de revisarse la situación de la firma digital y de los documentos electrónicos a nivel de Organismos Internacionales y del Derecho Comparado el informe realiza un análisis crítico del Boletín Nº2348-07. Por último, en un plano de *"lege ferenda"* o de ideas sobre cómo legislar el informe propone a la Comisión que por la vía de las indicaciones parlamentarias y del Ejecutivo se recoja un Proyecto de Ley elaborado por nosotros, más acorde a las necesidades que presentan el Comercio Electrónico tanto nacional como internacional de Chile y en aras de alcanzar un marco jurídico estable e idóneo que con certeza jurídica permita su desarrollo.

Contratos Informáticos

Autor: Dra. Catherine Ivette Mantilla Sánchez (Perú)
- Abogada egresada de la Universidad San Martín de Porres
- Grado Académico de "Maestro en Derecho" con especialidad en Derecho Civil y Comercial de la Universidad San Martín de Porres
- Diploma de Segunda Especialidad en Educación Superior de la Pontificia Universidad Católica del Perú.
- Fedatario Juramentado en Derecho Informático
- Se ha desempeñado como Asesora Consultora de los Consultorios Gratuitos del Colegio de Abogados de Lima y como Asesora Legal de la Notaría "Ramón Espinosa Garreta"
- Actualmente se desempeña como docente de Derecho Constitucional y Derecho Tributario en el Instituto Peruano de Administración de Empresas - IPAE.
- Asesora Legal Principal para el Banco Mundial en el Proyecto de Propiedad Informal

SUMILLA:

Al analizar el tema de Contratos Informáticos aparentemente nos encontramos frente a distintos tipos contractuales tradicionales y vigentes en la legislación tradicional como son la compra venta, locación, leasing, etc. , sin embargo al profundizar y al analizar el objeto, su naturaleza , podemos concluir que existe una tipología contractual específica y propia.

Los Contratos Informáticos son aquellos que establecen las relaciones jurídicas respecto de prestaciones consistentes en transferir la propiedad, el uso y /o goce de bienes informáticos y prestar servicios informáticos.

CONTRATOS INFORMATICOS

1.1 Concepto.-

Para hablar de los **contratos informáticos** primero daremos un concepto de los mismos, esto resulta algo difícil y complicado, más aún cuando no se ha llegado a conseguir una unidad de criterios por los diversos autores. Asimismo, el ritmo de desarrollo de la informática, el cuál es vertiginoso, genera su inadecuación al Derecho dado el carácter estático de éste último.

Quizás esta vaguedad con relación al concepto del contrato informático sea positiva ya que éste no se queda rezagado, frente al constante cambio, por el desarrollo tecnológico que la informática tiene.

Y es así como Daniel Altmark afirma que "... **es cierto que al analizar los contratos informáticos, aparentemente nos hallamos frente a distintos tipos contractuales tradicionales y vigentes en la legislación ordinaria, compraventa, locación, licencia, prestación de servicios, etc., a poco de profundizar ese análisis, y en atención particularmente a la especificidad de su objeto, pero también a la trascendencia de los contratos informáticos para la Empresa y el Estado, concluiremos en la necesaria estructuración de una tipología contractual específica y propia ...** "[1]

Como vemos los Contratos Informáticos sé confundieron con los contratos tradicionales, "**.. es así como la adquisición de un equipo computacional se asimiló a una compraventa de automóviles, la adquisición del software a un contrato de prestación de servicios y el de suministro de información al suministro de energía, etc. En su momento todo esto fue positivo; no obstante, se perdió de vista algo sumamente fundamental, pues en este tipo de acuerdos de voluntades es primordial clarificar extensamente cuál es el contenido del consentimiento de las partes que intervienen en ellos, puesto que, obviamente, quien adquiere un computador debe**

1 Altmark, Daniel Ricardo. Informática y Derecho Aportes de Doctrina Internacional. Volumen 1, Ediciones Depalma. Buenos Aires, p. 14, 1,987.

hacerlo teniendo presente cuál es la funcionalidad específica del equipo, el que sólo servirá en la medida que el software le dé sentido.

Dicho software, a su vez, tendrá sentido en la medida que a través de él se obtengan productos informáticos esperados y determinados a priori, y por último, dichos productos serán útiles en la medida que los datos en que se basen sean veraces, oportunos y conscientemente actualizados.."[2]

En base, a lo anterior podemos ver claramente que existe una verdadera complejidad, especificidad y trascendencia, en los contratos informáticos.

Como afirma Bonazzi, **"... A quien quiera servirse de la informática para ejercicio de su propia actividad se le presentan dos alternativas: dotarse de hardware y software para producir él mismo el servicio deseado, o bien acudir a quien ya dispone de aquellos para adquirir directamente el servicio. Frente a la primera hipótesis se estipularán uno o más contratos que darán lugar al "sistema contractual", mientras que en el segundo caso se hará normalmente la estipulación de un único contrato de "servicios".**

Hemos así individualizado las tres categorías fundamentales de contratos informáticos:

a) contratos de hardware
b) contratos de software
c) contratos de servicios.."[3]

A través, de lo anteriormente expuesto, queda establecido lo complejo que es conceptualizar un tema como el de los contratos informáticos; sin embargo, podemos afirmar que la normatividad peruana no los legisla, ni reglamenta convenientemente, por lo que el contrato informático queda comprendido dentro de la amplia definición del artículo 1351 del Código Civil " El contrato es el acuerdo de dos o más partes para crear, regular, modificar o extinguir una relación jurídica patrimonial".

Finalmente, para dar un concepto es conveniente tener en cuenta los bienes y/o servicios objeto de los contratos informáticos. Según Madeu "... **los bienes informáticos son un sistema y ese sistema lo constituye: a) las máquinas, b) los programas, c) el elemento humano que establece la interconexión de los elementos anteriores, d) La documentación (manuales, certificados etc.) y e) Asistencia técnica.."** [4]

Entonces, cada vez que nos encontremos ante un acto jurídico bilateral cuyo objeto sea alguno de los elementos mencionados anteriormente, estaremos en presencia de un contrato informático.

Los contratos informáticos los podemos definir como: aquellos que establecen las relaciones jurídicas respecto de prestaciones consistentes en transferir la propiedad, el uso y/o goce de bienes informáticos, y prestar servicios informáticos.

Los contratos informáticos constituyen la unión de contratos, es decir una gama de contratos, como compra venta, alquiler, leasing, llave en mano, licencia de uso, entre otros, en donde para transferir los bienes informáticos se unen más de un contrato.

Podemos señalar además que los contratos informáticos son innominados y como quiera que carecemos de una norma supletoria, por tanto al momento de redactar este tipo de contratos hay que ser cuidadosos. La complejidad se da especialmente en a) la especialidad de sus aspectos técnicos, b) la imprecisión del vocabulario técnico-jurídico y c) la estructura de los contratos. La falta de conocimientos técnicos dificulta la redacción e inter-

[2] Mayo de Goyeneche, Marie Claude. Informática Jurídica. Editorial Jurídica de Chile. Colección Cartillas Jurídicas, Santiago de Chile, p.110, 1,991.

[3] Madeu Martínez, Mario. Contratos Modernos. Revista Ius Et Veritas, Año II, No 3, Lima, Noviembre de 1,991.

[4] Correa, Carlos M. Derecho Informática. Ediciones Depalma, Buenos Aires, p. 154, 1,987.

pretación de este tipo de contratos, y en especial las principales cuestiones que se deben tomar en cuenta.

Por otro lado, el vocabulario informático sé caracteriza por el predominio de las palabras en idioma inglés, como por ejemplo, hardware, software, back-up, byte, etc. que muchas veces es de difícil comprensión.

Existe también complejidad porque no es fácil determinar los objetivos de los contratos informáticos que son según Flora M.de Katz, los siguientes: 1) establecer claramente la responsabilidad de cada una de las partes en la implementación del proceso, 2) establecer descripciones legales y técnicas claras que le permitan a las partes entender los términos de la relación, 3) establecer medidas cuantitativas de rendimiento factible, 4) establecer normas que contemplen posibles contingencias y su solución; por ejemplo, el caso fortuito y la fuerza mayor o cualquier otro hecho que pueda interrumpir la implementación e instalación del equipo, 5) establecer medios o recursos a los que se apelará en caso en que el sistema fracase.

En resumen, los contratos informáticos deben contemplar dos aspectos: 1) la descripción del trabajo a realizarse y el precio que se paga y 2) la regulación de las posibles contingencias, además el rendimiento y los plazos de entrega son puntos básicos que deben ser negociados y pactados cuidadosamente.

1.2 Clasificación de los contratos Informáticos

Para comprender los tipos de contratos informáticos realizaremos una clasificación de los mismos, queda claro que la misma es primordialmente con un fin didáctico.

1. Según Correa, los podemos clasificar según la materia del acto que se celebre, los contratos informáticos pueden corresponder a:

"..a) Equipamiento: unidades centrales de procesamiento, periféricos para la entrada y salida, o el almacenamiento de datos, equipo para comunicaciones, etc.

b) Software: software de base y aplicativo

c) Servicios: de análisis y diseño de sistemas, programación, adecuación de locales e instalación, capacitación, mantenimiento (de equipo de software), etc.

2. Por otro lado, los contratos informáticos pueden ser clasificados según el negocio jurídico que se celebre. Bonneau propone la clasificación siguiente:

a) El contrato de venta:
   - de equipo informático
   - de programas

b) El contrato de leasing:
   Las relaciones jurídicas se establecen entre el fabricante de material informático, la entidad financiera de leasing, y el usuario: entre el fabricante y la entidad financiera de leasing hay una compraventa, la entidad de leasing no utiliza el material y lo alquila al usuario juntamente con un compromiso de venta.

c) El contrato de locación:

   - de equipo
   - de programas

d) El contrato de horas - máquina: Éste es un contrato de cesión de uso en el cual el usuario sólo utiliza la máquina para una cantidad determinada de horas - máquina.

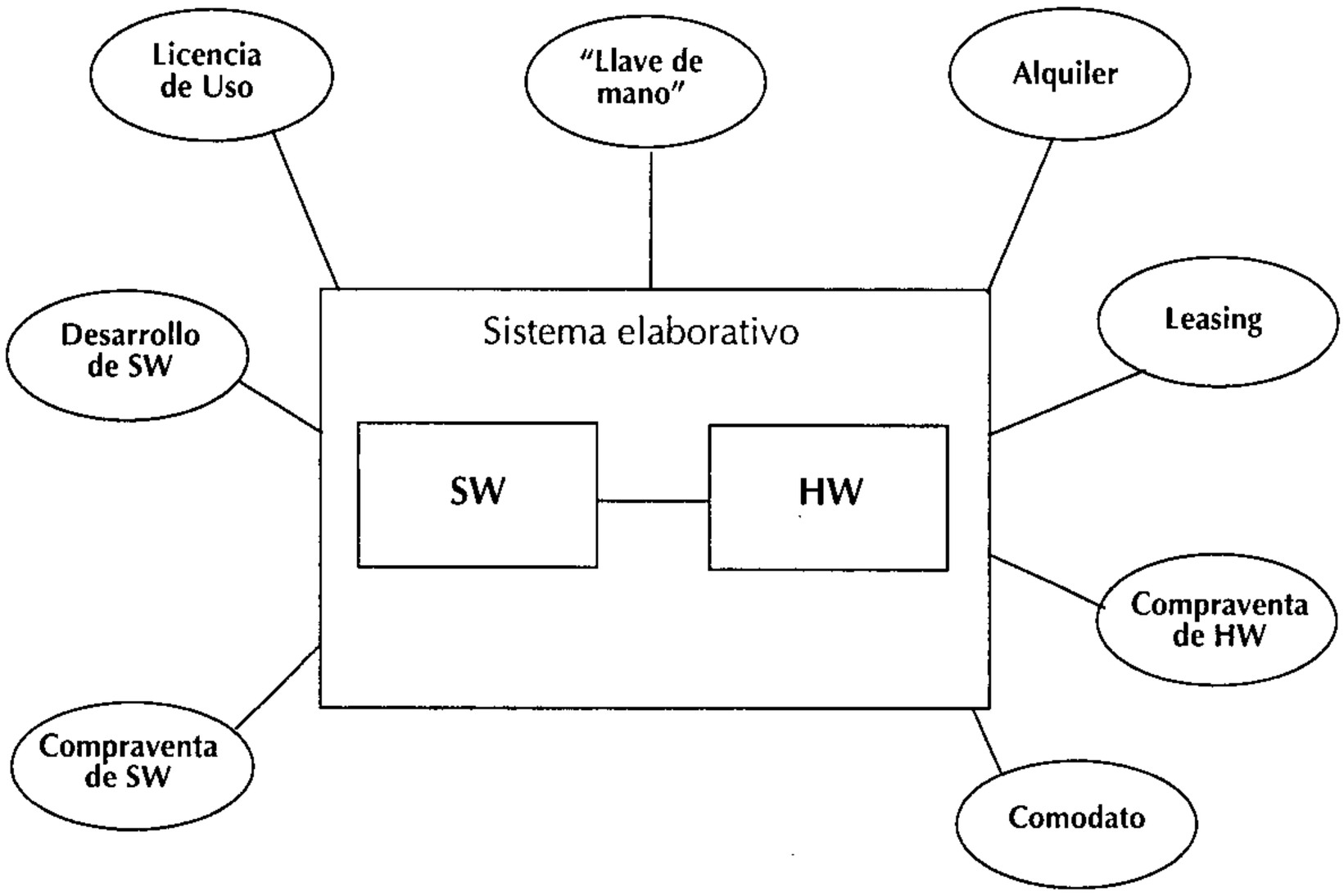
e) El contrato de mantenimiento

f) El contrato de prestaciones intelectuales, el cual comprende:
- los estudios previos,
- el pliego de condiciones
- la formación del personal
- el contrato de llave en mano

g) El contrato de prestación de servicios.."[5]

Bonazzi plantea otra clasificación afirmado que: **". Las relaciones hasta aquí examinadas, sin embargo, atañen a las amplias categorías contractuales, dentro de las cuales se encuentran acuerdos de diversa naturaleza jurídica. Así, por ejemplo, mientras que algunos componentes de hardware pueden ser adquiridos con contratos de contrato de compraventa, otros pueden ser adquiridos con contratos de alquiler o de leasing. Lo mismo vale para el software, que puede ser adquirido por licencia de uso o por medio de un contrato de desarrollo. Con referencia al hardware y al software se pueden presentar por lo tanto los tipos contractuales detallados en la figura ..."**[6]

Con esta figura queda establecido claramente los tipos contractuales o clasificaciones existentes más comunes, los cuales estudiaremos a través de la investigación.



[5] Correa, Carlos M.,Derecho Informático, Ediciones Depalma , Buenos Aires , pág. 154, 1987

[6] Bonazzi, Ermanno. Op Cit. p. 43.

Para finalizar daremos la clasificación de Flora M. de Katz, quien señala que: ". **Los tipos de contratos que pueden darse en el área de la computación son los siguientes:**

1) contratos de compra, locación o locación con opción a compra de hardware, es decir, máquinas, equipos dispositivos o soportes (físico); 2) contratos de compra o " leasing " de equipos periféricos, es decir, de los dispositivos utilizados por la unidad central como auxilio para entrada, salida o almacenamiento de información; 3) contratos de compra o "leasing" de terminales; 4) contratos sobre equipos de comunicación; 5) contratos de suministro; 6) contratos de provisión de equipos de protección y alarma; 7) contratos de software, comprendiendo tanto los programas que constituyen los sistemas operativos (software de base o logiciel de base) como los aplicativos (software aplicativo o logiciel d'application); 8) contratos de servicios de programación; 9) contratos de entrenamiento.."[7]

Como podemos apreciar existe una variedad de clasificaciones sobre los contratos informáticos, lo que permite y facilita su estudio e investigación.

1.3 El contrato Informático como un contrato de Adhesión.-

Los contratos informáticos asumen, con mucha frecuencia, la modalidad de contratos de adhesión, en donde una de las partes fija todas las cláusulas y la otra puede o no adherirse, sin poder negociarlas. Está característica es común en los contratos informáticos en donde los proveedores de material informático establecen su vínculo contractual con contratos preimpresos.

Hay que establecer que **".. El contrato por adhesión se halla inescindiblemente vinculado con la denominada sociedad de consumo, y ésta se relaciona a su vez, estrechamente, con la gran empresa y la acentuada tendencia a la producción en serie de bienes y servicios.**

El tráfico de masa se ve estimulado por la ampliación del número de consumidores, y éstos, a su vez -como en un operativo de reciclaje -, por la publicidad, la cual desenvuelta por los medios de comunicación social.."[8]

La economía moderna se caracteriza fundamentalmente por la celeridad del tráfico, donde la producción "standarizada" y en masa de bienes y servicios ha favorecido la difusión de un tipo particular de negociación orientada a permitir la rapidez de la circulación de productor y se adecua también al ritmo rápido de la vida moderna.

Como ya sabemos existe una producción masiva de bienes y servicios también un consumo masivo de bienes y servicios, haciéndose necesario un instrumento que permitía el tráfico de los mismos. Cabe señalar que este instrumento tiene que contemplar dos requerimientos que son su carácter masivo y la celeridad.

El concepto del contrato de adhesión es **".. aquel en que las cláusulas son dispuestas por uno de los futuros contratantes de manera que el otro no puede modificarlas ni puede hacer otra cosa que aceptarlas o rechazarlas, de tal suerte que este último no presta colaboración alguna a la formación del contenido del vínculo por un simple acto de aceptación o adhesión al esquema predeterminado unilateralmente.."**[9]

Con la finalidad de un mejor estudio, ahora analizaremos algo que es importante dentro de la contratación las " Cláusulas generales de los contratos" o " estipulaciones Generales".

"..Las estipulaciones generales de contratación aparecieron primeramente en los contratos de transporte marítimo y en los de seguro. Luego se presentan en las Bolsas. Se difunden más en el ramo de transportes. Des-

---

[7] Flora M. Katz. Contratos Informâticos. En Revista del Derecho Industrial. Ed. Depalma No 21, Búenos Aires, p. 509.

[8] Stiglitz-Stiglitz. Contratos por Adhesión. Cláusulas Abusivas y Protección al Consumidor. Ediciones Depalma, Buenos Aires. P. 47, 1.985.

[9] Stiglitz-Stiglitz, Op.cit. pág 50-52.

de fines del siglo XIX se introducen en las operaciones bancarias, luego son adoptadas en la "industria de abastecimiento" (agua, electricidad, teléfono) y pronto también en el movimiento de mercancías.

Las estipulaciones generales de contratación son, pues, una manifestación típica del Derecho de la economía moderna: realmente tiene sentido cuando una empresa realiza servicios o produce bienes de una manera sistemática y regular para el gran público, para una clientela indeterminada y actuando un tráfico en gran escala. A la realización de servicios en masa corresponde, como dice García Amigo, una contratación en masa.."[10]

Entonces podemos calificar a las cláusulas generales como el conjuntos de reglas que un particular (empresario, grupo o ramas de industriales o comerciantes) ha establecido para fijar el contenido (derechos y obligaciones) de los contratos que sobre un determinado tipo de prestaciones se propone celebrar. Por lo tanto elimina " a priori " los tratos previos entre las partes.

Establecido qué significa " Las Cláusulas generales de contratación", señalaremos las diferencias que existen con el contrato de adhesión, que constituyen para muchos la visión de un único fenómeno.

Hay que establecer que el artículo 1390 del Código Civil peruano declara que el contrato es por adhesión cuando una de las partes, colocada en alternativa de aceptar o rechazar íntegramente las estipulaciones fijadas por la otra parte, declara su voluntad de aceptar.

De La Puente y Lavalle afirma que se trata de **".. un contrato (obligatorio, desde luego) que requiere, por lo tanto, de oferta y aceptación. Además, la oferta no admite modificación alguna por el destinatario, quien sólo puede aceptarla o rechazarla en su oportunidad. Finalmente, este contrato se forma mediante la declaración de voluntad del destinatario de la oferta de aceptar ésta.**

Por otro lado las cláusulas generales de contratación, de acuerdo con lo que también se ha estudiado, son declaraciones unilaterales de voluntad del predisponente que no obligan a éste en el momento de redactarlas, pero que lo obligarán en el futuro cuando se incorporen a un contrato particular celebrado a base de ellas, resulta inadecuado compararlas con el contrato por adhesión dada la disparidad de sus respectivas naturalezas.

actor que puede incidir en el precio es la limitación de responsabilidades y obligaciones del predisponente. Sin embargo, se cuestiona si es legítimo este recurso pues, a la larga, puede resultar perjudicial para el cliente..."[11]

Entre los inconvenientes más usuales se encuentra la ambigüedad tanto en la forma como en el contenido de los contratos, existiendo muchas veces lagunas y cláusulas oscuras.

Si bien es cierto que podemos considerar a los contratos informáticos dentro de los contratos de adhesión hay que tener en cuenta las principales características de los contratos de adhesión que son:

" ..(1) Una de las partes es la que determina los términos de la relación contractual y elabora el esquema en forma previa, de modo que el destinatario está en la alternativa fatal de adherirse o no, esto, de celebrar o no el contrato.

(2) De acuerdo con lo expresado en el punto anterior, no existe capacidad o poder de negociación.

(3) El esquema planteado en la forma unilateral consiste en un conjunto de cláusulas o estipulaciones.

---

[10] De la Puente y Lavalle, Manuel " Estudios de Contrato Privado" Tomo I , Cultural Cuzco. Editores, Lima, pág. 300, 1983.

[11] De la Puente y Lavalle, Op. Cit, pág. 119-120.

(4) El destinatario de la propuesta, establecida como un complejo o todo unitario no es en términos generales un individuo determinado, sino un conjunto no precisado de personas frente a las cuales la propuesta se mantiene de modo duradero, independientemente de su aceptación o su rechazo .."[12]

Ahora analizaremos cada uno de los puntos anteriores con relación a los contratos informáticos los que pueden o no ser de adhesión.

(1) Es verdad que en los contratos informáticos existe una de las partes determina las condiciones del contrato, especialmente los proveedores de material informático, y el destinatario tiene la opción de celebrar o no el contrato.

(2) Con relación a este segundo punto creemos que sí es factible el poder de negociación en los contratos informáticos, sin embargo con relación a la compra venta de material informático es más difícil, se presentan dificultades en cuanto a que los proveedores son verdaderamente poderosos en el mercado de la industria informática. Por otro lado, con relación a los contratos de software y contratos de mantenimiento podemos plantear que sí es posible tener la capacidad de negociar, condiciones de entrega, plazos de entrega, garantías, cláusulas de responsabilidad, etc.

(3) Es cierto que el esquema planteado es unilateral, en donde una parte elabora las cláusulas o estipulaciones, mostrándose claramente en algunos contratos informáticos como es el de la compra venta de bienes informáticos.

(4) Cabe señalar que el destinatario de la propuesta es un grupo indeterminado de personas y se mantiene de esa forma independientemente de su aceptación o no, y en los contratos informáticos esto es plenamente aplicable pero en relación de los contratos informáticos de hardware.

Hoy en día nadie discute que los contratos de adhesión constituyen una modificación estructural de la contratación clásica, ahora se trata de una manera distinta de contraer obligaciones.

En conclusión creemos que la adhesión es un modo especial de contratar, pues en ella existe un acuerdo de voluntades eliminándose la etapa previa de la negociación, teniéndose en cuenta que la adhesión significa no discutir, lo que no significa no deliberar ya que siempre existe esta posibilidad .

Entonces podemos establecer claramente que los contratos informáticos son de adhesión en todos estos casos, aunque en muchas oportunidades asumen tales características especiales.

Por otro lado, en nuestra legislación no podemos hallar una respuesta satisfactoria al reto de la nueva tecnología, solamente en los aportes de la doctrina extranjera como la Argentina, Colombiana, Mexicana, Italiana.

Además, finalmente, implica una transformación en todo el Derecho, en donde una generación de nuevos objetos contractuales surge como una necesidad de la sociedad cambiante y moderna a la que el Derecho se debe adaptar, asumiendo el reto.

El contrato por adhesión está integrado por cláusulas que se denominan condiciones generales, cuyas notas más saltantes responden a la circunstancias de ser redactadas exclusivamente e íntegramente por una parte que adopta el nombre de predisponente. Además sé caracterizan por la estandarización de los instrumentos negociables que sirven a la comercialización y finalmente a su rigidez, elemento que apunta a la severa inmutabilidad de la fórmulas preordenadas. Pero también incluye condiciones particulares que las partes introducirán, conforme a la naturaleza del negocio celebrado, mediante los mecanismos tradicionales de formación del consentimiento.

[12] Arias Schreiber Pezet, Max. Exegesis, Tomo I, 2da. edición, Editores Studium, 1987.

Es evidente que la realidad de nuestros días nos enseña que existen innumerables negocios jurídicos, en donde las partes se vinculan mediante la adhesión de parte una de ellas a las estipulaciones que el mismo preredacta unilateralmente y la otra sólo puede aceptar o rechazarla. **".. La situación de desigualdad entre las partes, característica de los contratos de adhesión, se agrava en los contratos informáticos, no puede establecer juicio sobre el producto o servicio que se le propone. Por otra parte, desde el punto de vista económico su situación no le permite muchas veces resistir las presiones de los proveedores.."**[13]

Los Contratos Informáticos debido al desarrollo económico y tecnológico han modificado el modelo tradicional contractualista, pasando a ser una contratación en masa y despersonalizada, en donde existe una insuficiencia de los instrumentos jurídicos, ya que es difícil especificar los aspectos técnicos de los aspectos jurídicos. Además del uso de un vocabulario técnico - jurídico en la redacción de los contratos, por parte de los proveedores de bienes informáticos, los convierten en contratos de adhesión.

1.4 Naturaleza Jurídica de Los Contratos Informáticos.-

Si se desea estudiar bien el fenómeno de la informática éste debe ser hecho a través de la actividad contractual, así como del estudio de las relaciones contractuales entre los usuarios y proveedores de servicios de sistemas el mismo que se remonta en la actualidad a unos veinte años.

La palabra prestación se entiende aquí en un sentido muy amplio y puede significar la transferencia de un derecho sobre una "cosa" o la ejecución de una obra o de un servicio por parte del proveedor.

En el hecho de suministrar un equipo (hardware), alquilado o vendido, de poner a la disposición o ceder el derecho de uso de un programa (software), hay transferencia de un derecho de propiedad o de un derecho de uso limitado: se habla entonces de venta o arrendamiento respecto al hardware y de licencia o cesión de derechos o de uso o inclusive a veces de venta con respecto al software.

Un estudio, un servicio de asesoría, la realización de un programa específico, los trabajos informáticos sub-contratados, los servicios de mantenimiento de equipo, de producción de programas, la asistencia técnica o inclusive la formación, son prestaciones de servicio que se caracterizan por un hecho personal del proveedor dentro de un contrato de empresa.

En la doctrina no se ha establecido con claridad cuál es la naturaleza jurídica del contratos informáticos, suponemos que se trata de una aglutinación de modalidades de diversos contratos como compraventa, leasing, alquiler, llave en mano, Licencia de uso.

Asimismo, es un contrato completo que involucra en sus múltiples normas legales de distintas áreas de Derecho como el Derecho industrial, Derecho comercial, Derecho constitucional.

Hay que tener en cuenta de cada contrato informático se presenta en sí mismo su naturaleza jurídica propia sui generi diferente a los demás contratos.

Además afirma Lamerterie que **".. en los contratos informáticos se presentan dos gestiones: el recurso a los contratos tipos por una parte y a los contratos negociados, por otra. La negociación, cuando hay lugar a ella, obedece a diferentes factores:** la **importancia del contrato, el vínculo de fuerza los contratantes y en menor medida,** la **naturaleza del contrato hecho. Pero generalmente, el número de contratos y la analogía de las situaciones que ellos tratan, justifican económicamente una estandarización de los instrumentos y el recurso a los contrato tipo.."**[14]

Hay que Tener en consideración lo que afirma Vittorio Frosini, **"... la aparición de la computadora electrónica, sino también un bien económico nuevo, son sus características propias, que lo convierte a su vez en un productor de bienes nuevos, y que requiere una consideración jurídica específica. En efecto, la computa-**

---

[13] Correa, Carlos. Op. Cit. p. 155.

[14] De Lamberterie. Contratos En Informática, Revista Derecho y Tecnología Informática, Bogotá, p. 63-64, 1989.

dora electrónica acarrea modificaciones tanto en el campo de la programación industrial, como en el campo de la programación comercial, ya que abarca las bases mismas de los intereses económicos de las estructuras de producción de una sociedad industrial avanzada.

Crea una condición de vida económica totalmente nueva, porque crea un ambiente tecnológico nuevo en el mundo de los negocios, permitiendo un procesamiento de los datos cuya función es decisiva; pero él mismo es un objeto de producción nuevo con características originales, ya que sirve a dos tipos distintos de productores.."[15]

El contrato más usual con relación al hardware es la compra venta, también otros contratos como el Leasing aunque es menos debido a que los equipos informáticos se vuelven obsoletos muy pronto, por el gran avance tecnológico que existe en la industria informática, cabe señalar que los contratos de compraventa y leasing, son comunes en nuestro sistema legal peruano, no ocurren lo mismo con el contrato de software.

Con relación a la protección jurídica del software, lo primero que hay que tener en cuenta es que este es un fenómeno novedoso y como afirma Batto **".. Ante los ojos del jurista aparece como un nuevo objeto de derecho, capaz de producir importantes transformaciones sociales y económicas ...Algunos autores hablan de una naturaleza híbrida del software como conjunto de instrucciones consunstanciadas con un soporte físico.**

Otros entienden que el software no puede ser confundido con el soporte físico al cual se ha incorporado, ya que esas corporificaciones pueden ser de diverso tipo, tales como cintas, disquettes, tarjetas perforadas, etc. Es decir, no está sujeto a una estructura física determinada.

En el mismo sentido, también se ha señalado que el software tiene una creación, función y régimen independientes del hardware.." [16]

Enseguida analizaremos los caracteres jurídicos del contratos informáticos, entre los que podemos enumerar los siguientes:

1.- Es de Tipo Complejo, pues surge de una serie de vínculos jurídicos, ya que en ella podemos encontrar diversos contratos como sería compra venta de hardware y de software, leasing, licencia de uso de software, alquiler, contrato de servicios y mantenimiento. Posteriormente examinaremos cada de las relaciones mencionadas para comprobar su complejidad.

2.- Es un contrato atípico, puesto que carece de regulación propia, ya que en nuestro país no está regido por una normatividad legal especial. Empero en términos generales debemos este contrato se sujeta a los contratos tradicionales ya existentes y a las disposiciones generales establecidas en el Código Civil.

3.- Es un contrato principal, pues no depende de otro contrato que le sea precedente, es decir tiene " vida propia", en cambio puede suceder que vaya acompañado por garantía, sea estas reales o personales.

4.- Es oneroso, pues cada una de las partes, sufre un empobrecimiento, compensado por una ventaja. Además como sucede con otros contratos, esta onerosidad no significa necesariamente que exista equivalencia económica en las prestaciones y casi siempre existe un desequilibrio entre ambos.

5.- Es consensual, por aplicación de lo dispuesto en el artículo 1352 del Código Civil, sin embargo, en la práctica se celebra por escrito dada su trascendencia económica y de diferentes derechos y obligaciones que surgen como consecuencia de su nacimiento y normalmente la forma de celebración por adhesión, con cláusulas pre-redactadas con los llamados contratos tipo.

---

15 Frosini, Victorio. Informática Y Derecho, Editorial Temis S.A. Bogotá, p. 50, 1988.

16 Batto, Hilda N. Protección Jurídica del Software. Revista Derecho y Tecnología Informática. Setiembre, Bogotá, 1989.

Información y Derecho: el Desafío de su Integración

Autor : Patricia Reyes Olmedo (Chile)
Abogado Coordinadora de Proyectos Biblioteca del Congreso Nacional - Chile
Candidata a Doctor "Comunicación, Derecho de la Información
y Etica en America Latina y España". Universidad Complutense de Madrid

INTRODUCCION

En el mundo se ha producido una mutación profunda, difícil de comprender y analizar. La irrupción de la sociedad de la información constituye una revolución cultural, económica y social sin precedentes que ha impactado a todos los hombres y a todas las actividades.

Esta transformación se proyecta al Derecho, y de este modo, en cuanto Ciencia de la Información, puede afectar al objeto tradicional de la dogmática jurídica, contribuyendo al análisis y sistematización de los contenidos normativos de un ordenamiento jurídico. La ciencia de la información proporcionará las técnicas y herramientas necesarias para acceder a lo más elemental de la investigación del derecho, la norma jurídica, esto en atención a que el Derecho en cuanto fenómeno social pretende regular e influir en la conducta de los individuos, y con este fin se materializa en normas jurídicas que prescriben conductas, imponen deberes, que se manifiestan con carácter coercitivo.

La necesidad de información, tan común en cualquier orden de actividades hoy en día, resulta un imperativo cuando se trata de las normas jurídicas. La irrupción de la Ciencia de la información y las posibilidades ofrecidas por las modernas tecnologías nos obliga a revisar temas clásicos: Nos referimos a los mecanismos de publicidad del Derecho, la presunción de conocimiento de la ley, la seguridad jurídica como valor del Derecho, y la validez de conceptos como documento jurídico y lenguaje jurídico.

PUBLICIDAD DEL DERECHO

Sin lugar a dudas la publicidad de las fuentes formales del ordenamiento jurídico es un mecanismo efectivo de concreción de los principios del Estado de Derecho, como son la seguridad y certeza jurídica. Según Ducci Claro, "la publicidad pasó a constituir un presupuesto jurídico, un requisito para la validez o para la eficacia de las normas, apoyado en la necesidad de preservar la seguridad como valor"1.

Universalmente, el mecanismo establecido para dar a conocer la ley, es su publicación en un periódico que tenga el carácter de oficial.

En Chile, la exigencia de publicación tiene rango constitucional, el artículo 72 de la Constitución Política de la República de Chile, la prescribe como uno de los trámites en el proceso de formación de la ley, por lo que no puede omitirse. Por su parte la difusión de la ley se realiza mediante su inserción en el Diario Oficial de la República de Chile, según lo reglamenta en los artículos 6°, 7° y 8° el Código Civil de Chile. De acuerdo con lo establecido en el artículo 7° en su inciso tercero que dispone que "en cualquiera ley podrán establecerse reglas diferentes sobre su publicación", podría ocurrir que una ley señalará disposiciones especiales sobre su publicación en un órgano diferente.

Debemos sin embargo precisar que la publicación siendo una condición necesaria, no es suficiente para construir un sistema de acceso universal a las normas jurídicas. Este acceso se observa obstaculizado, entre otros aspectos por los siguientes:

1. El acceso regular al Diario Oficial es más bien reducido, aún dentro de los iniciados en el Derecho

2. Obviando el problema anterior, está el de recuperación de legislación generada en períodos anteriores al actual, en que recién se están generando esfuerzos para proceder a su almacenamiento electrónico.

3. La publicación de la legislación con un escueto y en ocasiones equívoco título.

Resulta por tanto ilusorio pretender restar relevancia al problema de la información en el Derecho, sosteniendo que ello está resuelto con la existencia de un órgano oficial que publica la nueva legislación. La inserción de las normas en una publicación oficial es tan sólo una labor de publicidad, que constituye el inicio del problema de la información de esas mismas normas, a aquellos a quienes se podrían aplicar.

PRESUNCION DE CONOCIMIENTO DE LA LEY Y EL ERROR DE DERECHO

En Chile, la presunción de conocimiento de la ley desde la fecha de su publicación en el Diario Oficial, le exige al ciudadano común estar informado de las normas jurídicas a las que se encuentra obligado. El artículo 7 del Código Civil Chileno dispone que "desde su publicación la ley se entenderá conocida de todos y será obligatoria". A su vez, el artículo 8° dispone que "nadie podrá alegar ignorancia de la ley después que ésta haya entrado en vigencia".

La afirmación que la autoridad de la ley se basa fundamentalmente en la presunción de conocimiento de la ley, es un pilar fundamental del ordenamiento jurídico. Sin embargo, como se ha señalado resulta imposible incluso al jurista conocer todo el Derecho vigente, imaginamos que también alguna área de éste.

Presumir que el Derecho es conocido por toda la comunidad parece ser una ficción, que no refleja la realidad, y que sólo puede entenderse a la luz de la necesidad de establecer la obligatoriedad de la norma jurídica, esto es, el carácter inexcusable de su cumplimiento.

Sin embargo, la normativa chilena vigente dispone en el inciso final del artículo 706 del Código Civil, que "el error en materia de derecho constituye una presunción de mala fe, que no admite prueba en contrario", aplicable a la situación en que se ha obrado en forma antijurídica, por un desconocimiento o un errado conocimiento de la ley. Es preciso sin embargo, declarar que tanto en el plano civil como en el penal hay voces que se han alzado frente a estas interpretaciones. En el plano civil, se ha señalado que "bajo la denominación *presunción del conocimiento de la ley* se engloban principios de distinto alcance. Uno de ellos es la obligatoriedad, es decir, la ficción de conocimiento de la ley que hace inexcusable su incumplimiento. Pero otro problema muy distinto es la influencia que sobre los actos jurídicos pueda ejercer el error de derecho. La ignorancia del derecho no puede servir de pretexto para eludir su observancia, pero puede tener una influencia cuando sea alegada como presupuesto de aquellos hechos de que la ley hace derivar consecuencias jurídicas"[2]. Por su parte, contemporáneamente la generalidad de la doctrina penal, bajo el nombre de error de prohibición, concede valor al error de derecho y concluye que, debidamente acreditado en el proceso, debe conducir a la absolución del reo, por faltar uno de los elementos del delito cual es la culpabilidad, en su aspecto de conciencia de la ilicitud.

Así la ciencia del Derecho no puede permanecer ajena a las conclusiones reseñadas, y ya las modernas teorías integran a su ámbito un problema hasta ahora inexistente: la legitima posibilidad de exculparse de una conducta antijurídica por un desconocimiento de las leyes que la regulaban.

Sin embargo, una interpretación irrestricta de la norma del artículo 706, vislumbra el problema que enfrenta el Derecho y la necesidad que éste tiene de generar métodos y fórmulas, que permitan hacer realidad la ficción de conocimiento de la ley.

---

[1] CARLOS DUCCI, Derecho Civil, Parte General. Cuarta Edición, Editorial Jurídica de Chile, Santiago, 1995, pág. 59.
[2] JOSE LUIS DE LOS MOZOS, Derecho Civil Español. Salamanca, 1977, Vol. I, pág. 675, y JOAQUIN COSTA, La ignorancia del derecho. Europa-América, 1957.

SEGURIDAD JURIDICA

La seguridad jurídica es un principio fundamental del Derecho, y se expresa cuando el individuo como sujeto activo y pasivo de relaciones sociales, sabiendo y debiendo saber cuáles son las normas jurídicas vigentes, tiene fundamentadas expectativas que ellas se cumplan[3].

Este valor puede concebirse de dos maneras:

Seguridad jurídica propiamente tal, que es la seguridad del individuo frente a todo lo que atente contra sus derechos, que otros conciben como la certidumbre fundada y garantizada que la norma será cumplida.

Certeza jurídica o certeza del Derecho, que es la perceptibilidad cierta de la norma jurídica, la certidumbre de que se trata del contenido del Derecho vigente, situación que precave al ciudadano de las modificaciones arbitrarias de este Derecho.

La certeza jurídica, requiere de cuatro condiciones, en opinión del profesor Jaime Williams[4]:

1. Que el Derecho sea positivo

2. Que la norma preexista a la conducta regulada por ella

3. Que la norma sea conocida, así como las consecuencias de su incumplimiento

4. Que la norma sea inteligible, es decir carezca de ambigüedad que pueda dar lugar a equívocos.

Es en este aspecto de la certeza jurídica en que se observa la necesidad que tiene la Ciencia del Derecho de las Ciencias de la Información. Las condiciones o requisitos de la certeza hacen indispensable contar con herramientas e instrumentos que permitan al ciudadano acceder en forma oportuna y precisa a la información y alcanzar el conocimiento de las normas jurídicas del ordenamiento respectivo.

A nuestro juicio, para el logro de este objetivo cada sistema debe contemplar:

a) Difusión de cada uno de los trámites y actividades del proceso legislativo y más tarde de la ley promulgada. Los textos de las iniciativas (proyectos de ley), actas de las sesiones, informes de comisiones deben ser ampliamente difundidos a la opinión pública.

b) Información sobre el ordenamiento jurídico en su conjunto. Este objetivo requiere la máxima atención, en atención a la complejidad que reviste su consecución. Como hemos señalado anteriormente es difícil incluso al experto llegar a conocer el derecho vigente respecto de ciertas materias, y dado que esas normas pueden ser el objeto de discusión en un proceso jurisdiccional, el problema de la información constituye un problema de la Ciencia del Derecho y se transforma por tanto en factor decisivo de la existencia de seguridad jurídica en los ordenamientos jurídicos.

DOCUMENTO JURIDICO

Revisaremos este concepto a fin de darle contenido a partir de la introducción de las modernas tecnologías de información. En efecto, la expresión documento jurídico puede inducir a relacionar a todo documento que tenga alguna relevancia para el Derecho, pero esta interpretación llevaría a hacer términos equivalentes documento y documento jurídico, toda vez que cualquier documento puede llegar a tener una importancia en

---

[3] JORGE MILLAS. Filosofía del Derecho. Editorial Publilex, Santiago, 1970, Pág.225

[4] JAIME WILLIAMS. La Seguridad como Valor del Derecho. Universidad de Chile, Santiago, 1983, pág. 29.

el derecho, por ejemplo como medio probatorio en un proceso, donde incluso puede llegar a ser el objeto mismo de la controversia.

De este modo, intentaremos precisar que documento jurídico es un concepto más específico que documento relevante para el Derecho.

Conceptualizaremos entonces el Documento Jurídico como aquel "soporte físico que se caracteriza por poseer información jurídica, sea ésta una norma jurídica de cualquier jerarquía o una explicación científica, interpretación, recopilación o una sistematización de su contenido jurídico, o el resultado de investigaciones empíricas acerca de la vigencia real o práctica del Derecho".

Así concebido el documento jurídico se caracteriza por:

1. Ser una expresión o manifestación de una norma jurídica, o una elaboración sobre ella.

2. Contener una validez casi permanente, en cuanto interesa no sólo al Derecho vigente, sino también al que tiene un carácter histórico.

3. Utilizar un lenguaje técnico que se denomina lenguaje jurídico.

Por su parte, los documentos jurídicos, abundantes y extensos, requieren una organización y procesamiento que permita su búsqueda y recuperación, de manera eficiente y eficaz.

El desafío por tanto es enorme, por cuanto la oportunidad y exactitud en la información jurídica resulta del todo indispensable para el adecuado desenvolvimiento de la vida social y jurídica. Esto viene inquietando desde hace ya algún tiempo a los juristas del mundo entero. En Chile, don Fernando Fueyo, ha reflexionado sobre este tema y señalado: "¿Qué autor en materia jurídico social podría escribir hoy con mediana honestidad y para que su escrito sea útil, sin una información amplia, integrada, equilibrada, moderna, comparada, a la cual pueda tener fácil acceso? ...Faltando información estaremos ante un investigador irresponsable y aventurero[5].

A la vista de esta y otras reflexiones resulta claro que se requiere mejorar los sistemas de almacenamiento, procesamiento y recuperación de los documentos jurídicos generados, a fin de lograr el desarrollo de la Ciencia del Derecho.

LENGUAJE JURIDICO

El derecho pretende regular la vida del hombre en sociedad, desea orientar sus conductas con miras a la obtención de ciertos objetivos: la paz social, la justicia, la libertad y la seguridad jurídica. Estos mandatos deben tener una forma, un canal que los haga comprensibles y asimilables a sus destinatarios. De ahí, que la interrelación entre lenguaje y norma jurídica es indiscutible. El lenguaje por tanto sirve de intermediario entre el normador y el normado. Pero aún podemos decir más, pues el lenguaje no sólo es el comunicador de los mensajes normativos, sino que el Derecho es lenguaje, y no existe Derecho si no lo es. Se ha señalado así que "la diferencia existente entre una ley física y una norma jurídica radica en que, en tanto la primera es rige antes de su enunciación, la norma jurídica, en cambio, requiere ser enunciada lingüísticamente para que pueda identificarse y actuar"[6].

---

5 FERNANDO FUEYO LANERI. Teoría y Práctica de la Información Jurídica. José Bushatsky Editor, Sao Paulo, 1977, pág. 16.

6 MIGUEL SANCHEZ MAZAS, Algebra del Derecho y procesamiento de la Legislación. Jornadas sobre Lógica, Informática y Derecho, España, 1984, pág. 203.

Todas las disciplinas científicas son interdependientes, lo mismo acontece con el Derecho. Si consideramos además que éste regula las variadas situaciones de la vida del hombre observaremos que siendo un lenguaje científico el lenguaje de la norma jurídica debe utilizar como herramienta insustituible el lenguaje común, así como el lenguaje técnico de otras ciencias o artes.

De este modo, podemos decir que el lenguaje utilizado en los documentos jurídicos comprende:

a) Lenguaje estrictamente jurídico, es decir de particular y exclusivo uso en el mundo jurídico, como por ejemplo, resciliación, comodato, fideicomiso.

b) Lenguaje técnico especializado de otras disciplinas o de otras ciencias, por ejemplo radioactividad, electroencefalograma, parto

c) Lenguaje común como noche, día.

El lenguaje jurídico tiene elementos propios y característicos, pero no podemos dejar de señalar que presenta dificultades que generan incertidumbre, variedad de interpretaciones que terminan socavando el principio de igualdad ante la ley. Entre las principales dificultades observadas se encuentran:

1. Mala estructuración

2. Ambigüedad sintáctica y semántica

3. Incoherencia y contradicciones internas

4. Incompletitud, lo que genera verdaderas lagunas legales

5. Redundancia

Las causas son variadas, entre las más reiteradas podemos destacar: las decisiones de política contingente, el excesivo uso de un lenguaje común que presenta ambigüedad (variadas significaciones para una misma palabra), y la insuficiencia de desarrollo de la técnica legislativa, por considerarla poco relevante, situación que permitiría eliminar redundancia, contradicciones y falencias en la composición estructural del lenguaje de las normas jurídicas.

Un ejemplo en que el legislador chileno ha empleado mal la técnica, pues designa erróneamente el género lo encontramos en los artículos 93 y 94 del Código Civil Chileno, que se refieren a la "rescisión del decreto de posesión definitiva de los bienes del desaparecido".

El vocablo rescisión remite a lo señalado en el artículo 1.680 del Código Civil Chileno "La rescisión o nulidad relativa es una sanción legal que se aplica a los actos o contratos en que falta alguno de los requisitos que la ley prescribe para el valor de ellos, en atención a la calidad o estado de las personas que los ejecutan o celebran". Pero ocurre que el referido decreto de posesión definitiva no adolece de vicio alguno de nulidad relativa, ya que ha sido dictado por el juez, observándose todos los requisitos de validez exigidos por la ley para las resoluciones judiciales. Se trata de un acto procesal plenamente válido, y lo que permite que sea dejado sin efecto es la circunstancia que el presunto muerto ha aparecido, faltando por tanto, el supuesto para su dictación. En tal caso, el legislador debió hablar de revocación y no de rescisión.

A la luz del ejemplo anterior, se justifica plenamente la incorporación de un lenguaje de auxiliar con carácter normalizado, que elimine la incertidumbre, rescate la totalidad de los conceptos involucrados en un documento jurídico, de manera tal de obtener su total y oportuna recuperación. A este efecto, resulta nuevamente indispensable la colaboración de la Ciencia de la Información que ha desarrollado en profundidad la creación de Listas de Materias o Tesauros para bases de datos especializadas.

A MODO DE CONCLUSION

Una vez expuesto los problemas a que se enfrenta el Derecho en la nueva sociedad de la Información, es que creemos que la información ha pasado a formar parte del objeto de la ciencia del Derecho. La información jurídica y los medios para acceder a ella ya no sólo deben interesar al jurista como auxiliares de su labor, sino que ahora también forman parte de su objeto de estudio para determinar que posibilidades concretas tiene el ciudadano de conocer la normativa que lo rige.

De este modo se puede integrar plenamente la Ciencia de la Información a solucionar problemas que se le plantean a la Ciencia del Derecho, sin que por cierto, cada una pierda su identidad.

En conclusión la Ciencia de la Información puede brindar auxilio al desarrollo del Derecho, al generar nuevas perspectivas para observar instituciones clásicas de nuestro Sistema Jurídico.

Los servicios de certificación

Ingnacio Alamillo y María Pérez (España)

1.1. LA FIRMA ELECTRONICA

La firma electrónica es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge (art. 2.a RDL 14/99).

Las transacciones firmadas en cumplimiento de la ley tienen garantizada plena validez y efectos jurídicos.

El art. 3.1 establece que la firma electrónica [cuando cumpla determinados requisitos] tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

La firma electrónica se encuentra reconocida en España por el Real Decreto Ley 14/1999, de 17 de septiembre, establece, en su art. 1:

"Artículo 1. Ámbito de aplicación.

1. Este Real Decreto-Ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-Ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones."

1.2 LA FIRMA ELECTRONICA LEGAL

Una firma electrónica legal es una firma electrónica avanzada que cumple determinados requisitos adicionales, como garantía de su calidad.

Una firma electrónica avanzada es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos (art. 2.b).

Esta firma electrónica debe basarse en un certificado reconocido, aquél que contiene determinadas informaciones (art. 8) y que ha sido emitido respetando determinadas cautelas (art. 12). El certificado reconocido tiene que haber sido expedido por un prestador de servicios de certificación acreditado (art. 6).

Finalmente, esta firma electrónica tiene que haber sido generada empleando un dispositivo seguro de creación de firma (art. 19) debidamente certificado (art. 6).

Cuando deseamos que determinados actos tengan determinados efectos, debemos emplear la forma escrita. Lo mismo sucede en muchos casos, en los que esta forma escrita no es necesaria, pero acudimos a la misma para documentar debidamente el acto en cuestión, y disponer de un medio de prueba.

Lo mismo sucede en el mundo digital, y existen muchos medios técnicos para probar las transacciones

(los actos) que se producen en el mismo: identificador de usuario y contraseñas, registros de transacción en bases de datos, etc.

Sin embargo, sólo existe una tecnología que nos garantiza ese medio de prueba equivalente al documento firmado, en el mundo digital: la firma electrónica legal; es decir, la firma electrónica que cumple los requisitos establecidos en el RDL 14/1999, de 17 de septiembre.

Por este motivo, siempre que deseemos tener un equivalente del documento escrito en el mundo digital, debemos emplear firma electrónica. Y si queremos que esa firma sea incuestionable, debe tratarse de una firma electrónica legal.

1.3 EFECTOS DE LA FIRMA ELECTRONICA LEGAL

La firma electrónica legal es la única que, además de ser válida, tiene efectos jurídicos plenos (art. 3.1).

Esto significa que la firma electrónica legal tiene, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.

La firma electrónica simple es la firma electrónica que no cumple todos los requisitos que establece el RDL 14/1999, firma que es válida, pero no tiene efectos automáticos. De este modo, dice el art. 3.2 que "a la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica".

Emplear firma electrónica simple supone el riesgo legal de tener que demostrar en juicio (o arbitraje) la corrección de la firma y su seguridad, prueba que puede llegar a ser inviable, por lo que siempre se recomienda emplear firma electrónica legal, que, además de válida, es efectiva de forma automática.

1.4 REQUISITOS LEGALES PARA DAR VALIDEZ A UNA FIRMA ELECTRONICA

El único requisito que se establece es que se trate de una firma electrónica que garantice lo establecido en el art. 2.a: "conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge".

Sin embargo, esta definición excluye que un PIN sea una firma electrónica, por los siguientes argumentos:

1. No puede defenderse que el PIN permita la creación de firmas electrónicas; ni que exista vinculación entre documento y firma electrónica, ni que sea detectable la modificación de los datos "firmados" con el PIN.

2. El artículo 2, d) establece que los datos de creación de firma "son los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica". No puede defenderse que el PIN sea un dato único, ni desde luego una clave criptográfica privada, para crear firma electrónica alguna.

3. El artículo 2, g) establece que los datos de verificación de firma "son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica". No puede defenderse que el PIN, aún si se considerase clave criptográfica privada (absurdo), tenga su correlativa clave pública para verificar las firmas creadas con el mismo (imposible técnicamente).

   Como puede verse, ni PIN ni firma electrónica simple tienen efectos directos; el primero de ellos ni siquiera tiene validez como firma electrónica. Sólo la firma electrónica legal tiene validez y eficacia jurídica plena.

1.5 LOS CERTIFICADOS DIGITALES, ELEMENTO ESENCIAL DE LA FIRMA ELECTRONICA

Un certificado es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad (art. 2.i).

El certificado contiene en su interior los datos de verificación de firma (los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica – art. 2.g).

En el caso de la firma electrónica basada en criptografía asimétrica (la más extendida en la actualidad, también denominada firma digital), los datos de verificación de firma tienen una correlación matemática con los datos de creación de firma (los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica – art. 2.d).

Cuando recibo un mensaje de correo firmado electrónicamente, debo realizar algunas comprobaciones antes de confiar el mensaje, comprobaciones que suelen ser automáticas.

Comprobaré los siguientes aspectos:

1. Que la firma electrónica es avanzada
2. Que se basa en un certificado reconocido
3. Que el prestador que ha expedido el certificado se encuentra debidamente acreditado
4. Que la firma ha sido generada con un dispositivo seguro de creación de firma
5. Que ese dispositivo de creación de firma electrónica se encuentra debidamente certificado

Cuando haya comprobado estos cinco extremos, comprobación que, como ya se ha dicho, suele ser automática, entonces podré confiar en la firma electrónica, el signatario y el mensaje firmado.

Una firma electrónica avanzada es un conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos (arts. 2.a y 2.b).

Los medios que el signatario mantiene bajo su exclusivo control son los datos de creación de firma electrónica, como nos muestra la definición de signatario: persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa (art. 2.c). Y el dispositivo de creación de firma es un programa o un aparato informático que sirve para aplicar los datos de creación de firma (art. 2.e), siendo éstos los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica (art. 2.d).

Como sabemos, existe una relación matemática entre los datos de creación de firma (la clave privada) y los datos de verificación de firma (la clave pública), que son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica (art. 2.g).

Pues bien, un certificado es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad (art. 2.i). Sin certificado no podríamos, por lo tanto, verificar la firma electrónica, de donde viene esta relación.

1.6 TIPOLOGIA DE CERTIFICADOS DIGITALES

En principio, pueden existir innumerables tipos de certificados, dependiendo de la voluntad de los diferentes prestadores de servicios de certificación, que pueden consignar dentro de cada certificado las informaciones que consideren necesarias.

Sin embargo, el RDL 14/1999 se plantea la existencia de dos tipos de certificados:

1. El certificado ordinario

2. El certificado reconocido

El certificado ordinario es la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad (art. 2.i), pero que no cumple ningún criterio de calidad, motivo por el cual la ley no otorga efectos jurídicos plenos a las firmas electrónicas que se basan en estos certificados.

Por el contrario, el certificado ordinario, que se define como el certificado que contiene la información descrita en el artículo 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el artículo 12 (art. 2.j), es un certificado en el que se pueden basar firmas electrónicas con efectos jurídicos plenos (teniendo en cuenta que deben cumplirse también los restantes requisitos legales).

Respecto a los certificados reconocidos, el art. 8 establece algunas reglas respecto a su contenido:

a. La indicación de que se expiden como tales.

b. El código identificativo único del certificado.

c. La identificación del prestador de servicios de certificación que expide el certificado, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.

d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e. La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca.
Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquel dé su consentimiento.

f. En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

g. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario

h. El comienzo y el fin del periodo de validez del certificado.

i. Los límites de uso del certificado, si se prevén.

j. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Por otra parte, la consignación en el certificado de cualquier otra información relativa al signatario, requerirá su consentimiento expreso.

1.7 REGLAS APLICABLES AL SERVICIO DE FIRMA ELECTRONICA

Una política es una forma de controlar el intercambio de mensajes, dentro de un determinado entorno; la política se compone de reglas orientadas a administrar el intercambio de información entre dos partes, dentro del entorno que hemos mencionado anteriormente.

La política puede establecer el significado que se otorga a cada mensaje por el que se intercambia información, permitiendo la existencia de transacciones, puesto que una transacción no es otra cosa que una forma de intercambio de mensajes cuyos significados y consecuencias han sido establecidos por una política administrativa.

Para que una transacción pueda considerarse fiable, tiene que ser segura; esto es, tiene que haber tenido lugar dentro de un entorno de seguridad debidamente administrado por un dominio reconocido por ambas partes.

Cuando se emplea un certificado para hacer fiable una transacción, los elementos de la política de seguridad en cierto modo se incluyen y asocian al certificado. De este modo, tenemos una política de certificado.

Es importante elegir un certificado cuya política garantice, al menos, los aspectos obligatorios que la ley exige a los certificados reconocidos, especialmente cuando redactamos nuestra propia política de firma electrónica.

Por su parte, una política de firma electrónica en un conjunto de reglas que rige la firma electrónica, en los siguientes y otros aspectos:

1. Identificación de la política de firma electrónica
2. Formato de la firma electrónica
3. Intención del signatario
4. Certificados reconocidos que se emplearán
5. Otros atributos que se emplearán
6. Sellos de tiempo que se emplearán

Gracias a la política de firma electrónica, podemos adaptar este potente mecanismo de seguridad con reconocimiento jurídico a nuestras necesidades administrativas, organizativas, negociales o comerciales.

Los anteriores extremos han sido establecidos por el Instituto de Normalización Europeo de Telecomunicaciones, por encargo de la Comisión Europea, al objeto de crear normas aplicables al desarrollo de la firma electrónica legal que se recoge en la Propuesta de Directiva y en el Real Decreto-Ley español.

2. ESTATUTO DEL PRESTADOR DE SERVICIOS DE CERTIFICACION

2.1 La figura del prestador de servicios de certificación

Un prestador de servicios de certificación es la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica (art. 2.k).

Los prestadores de servicios de certificación generan los certificados digitales, motivo por el cual el RDL establece un sistema general de supervisión de su actividad, un conjunto de obligaciones que deben cumplir cuando expidan certificados reconocidos al público y un régimen administrativo sancionador que se aplicará cuando no apliquen la diligencia debida en sus operaciones.

En muchos casos, el prestador de servicios de certificación va a ofrecer otros servicios, además de la expedición de certificados: por ejemplo,

1. Prestará servicios de registro
2. Entregará los dispositivos seguros de creación de firma electrónica
3. Ayudará a definir los sistemas que empleen firma electrónica
4. Ayudará a construir o suministrará los dispositivos de verificación de firma electrónica
5. Prestará servicios de validación de certificados y firmas electrónicas
6. Aportará tecnologías de sellos de tiempo

El RDL considera necesario que la firma electrónica disponga de plenos efectos jurídicos, siempre y cuando la misma cumpla unos criterios de calidad.

Siendo el certificado uno de los elementos clave para la firma electrónica, el RDL establece todo un conjunto de obligaciones a los prestadores de servicios de certificación; especialmente:

1. La generación de certificados, para los que basta con el mantenimiento de niveles de calidad ordinaria
2. La generación de certificados reconocidos, que requieren el mantenimiento de niveles de calidad superior

2.2 Actividades típicas del prestador de servicios de certificación

Los prestadores de servicios de certificación suelen ofrecer múltiples servicios, desde la expedición de certificados hasta la validación de firmas electrónicas, pasando por la operación de directorios y entrega de dispositivos de firma electrónica.

De acuerdo con la Propuesta de Directiva de la Unión Europea sobre firma electrónica, todas las entidades que prestan estos servicios se denominan prestadores de servicios de certificación, aunque el criterio seguido en la ley española es claramente diverso.

A los efectos que ahora perseguimos; esto es, exponer las actividades básicas del prestador, diferenciaremos las funciones de Autoridad de Certificación y Autoridad de Registro, también denominada, en ocasiones, Entidad de Registro Colaboradora. A este efecto, por ejemplo, en las Prácticas de Certificación de la Agencia de Certificación Electrónica, S.A. se establecen las siguientes tareas, para cada una de las anteriores entidades:

"1.3.1 Autoridades de Certificación

Las presentes prácticas se aplicarán a ACE en la emisión y gestión de certificados dentro de sus servicios de certificación pública. También serán de aplicación a las entidades de emisión dentro de la jerarquía de ACE que no dispongan de prácticas propias. Se entiende por entidad de emisión dentro de la jerarquía de ACE aquélla para la que ACE genera certificados, firmando en su nombre. Esta circunstancia figura en el certificado generado para la entidad de emisión que se encuentra dentro de la jerarquía de ACE.

Cuando emplee esta C.P.S. en su emisión de certificados, la entidad de emisión será la única obligada frente a todas las partes intervinientes en la misma, ocupando la posición que en estas prácticas ostenta ACE.

ACE podrá emplear una o más Autoridades de Registro para realizar determinadas funciones, como se expone a continuación.

1.3.2 Autoridades de Registro

Estas prácticas se aplican a las Autoridades de Registro que ACE emplee en los procedimientos de emisión y gestión de certificados. Estas entidades se denominan también Entidades de Registro Colaboradoras (E.R.C.).

Las autoridades de registro son normalmente entidades diferentes de suscriptores y solicitantes de certificados, que realizan las funciones descritas a continuación, actuando en nombre y por cuenta de ACE, asumiendo las obligaciones y responsabilidades que se especifican en las secciones 2.1.2 y 2.2.2 de esta C.P.S. Las autoridades de registro deben superar un procedimiento previo de homologación que garantiza su fiabilidad.

1.3.2.1 Funciones

Las autoridades de registro pueden realizar las siguientes tareas:

- validar solicitudes de certificado en base a determinados procedimientos de identificación, apropiados a los niveles de seguridad que ofrece cada categoría de certificado. Las autoridades de registro realizan las peticiones de generación de certificados y ACE emite los certificados a los suscriptores. ACE podrá tener más de una autoridad de registro, y
- entregar físicamente los certificados a los suscriptores, en disquete u otro medio idóneo para ello.

1.3.2.2 Procedimientos

Para proceder a la validación de la solicitud, las AA.RR. deberán emplear los procedimientos descritos en la sección 4.1.2 de esta C.P.S. para cada categoría y, en su caso, tipo de certificado.

La A.R. no podrá emplear otra A.R. para realizar sus funciones, de modo que siempre tratará físicamente con el solicitante y, en su caso, suscriptor de certificados.

1.3.2.3 Homologación y documentación

Toda A.R. debe ser homologada por ACE como paso previo a su entrada en funcionamiento, para sus operaciones dentro de cada categoría de certificados. Las condiciones de homologación se establecen, para cada versión de la C.P.S., en el documento denominado "Procedimiento de Homologación de Autoridad de Registro", que se suministrará a las entidades interesadas que remitan una comunicación en tal sentido a ACE, tal como se especifica en la sección 2.4.4 de esta C.P.S. La citada petición deberá indicar la categoría o categorías para las cuales desee homologarse la A.R.

La A.R. deberá tener a disposición de solicitantes y, en su caso, suscriptores de certificados, un documento denominado "Prácticas de Registro", que especifique sus procedimientos operativos y de garantía de la seguridad."

2.3 Establecimiento y ley aplicable al prestador

El prestador de servicios de certificación deberá radicar su domicilio social, es decir, establecerse dentro del ámbito geográfico nacional. Además, deberá cumplir con el requisito del artículo 7 del RDL 14/1999 relativo a la inscripción de la empresa en un registro especial.

Esto será lo que determine su ley aplicable. Sin embargo hay que tener en cuenta la relevancia transnacional de las actividades que realizan, puesto que el PSC puede haberse establecido en España, según el ordenamiento jurídico español, y tener un cliente alemán que utiliza el certificado español para sus relaciones con una empresa guatemalteca. Podría así suscitarse la duda de cuál será la ley aplicable a los litigios que surjan relacionados con el certificado emitido por el PSC español; la respuesta parece clara, resultará preferible que sea siempre la ley aplicable al PSC, con independencia del lugar de emisión del certificado.

Esta solución se encuentra en consonancia con la futura Directiva de la Unión Europea de Comercio Electrónico, que establece, para los servicios de la sociedad de la información, el régimen general de aplicación de la ley del país de origen. Este criterio no constituye, como es sabido, una norma de conflicto, sino una regla de localización, que permite aplicar la normativa interna de ese Estado.

La definición de servicio de la sociedad de la información ha sido recientemente introducida en España, a través del Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información, en transposición de la Directiva 98/48/CE, del Parlamento Europeo y del Consejo, de 20 de julio, que modifica la Directiva 98/34/CE, ampliando su campo de aplicación a los reglamentos relativos a los servicios de la sociedad de la información.

El empleo de los puntos de conexión tradicionales en materia contractual permite acudir a las dos soluciones que en esa Propuesta de Directiva se contemplan: la de aplicar la legislación propia del Estado donde se encuentra establecido el prestador o bien aplicar, a elección del prestado, la ley de destino. En el primer caso, habrá que corregir la ley del Estado de establecimiento del prestador con las normas materiales imperativas del Estado de destino, únicamente cuando el suscriptor resulte ser un consumidor (cfr. Artículo 5 del Convenio de Roma de 1980); en los restantes casos, los más frecuentes en la práctica actual, la relación se establece entre dos empresas, por lo que se somete la relación de forma íntegra, y sin factores de corrección, a la ley del Estado de establecimiento, como hemos indicado anteriormente.

2.4 El Registro de prestadores

Este Registro, de nueva creación, depende del Ministerio de Justicia. Su misión es la de proporcionar información sobre los PSC y tener un seguimiento más o menos cercano de las actividades que vienen desarrollando.

Así pues, en este Registro, que todavía no se encuentra en funcionamiento, deberán inscribirse todas y cada una de las personas físicas o jurídicas que se dediquen a la prestación de servicios de certificación siempre y cuando tengan su sede en el territorio español antes del comienzo de su actividad, y como medida transitoria, la ley concede un plazo de un año para la primera inscripción a aquéllos prestadores que ya estuvieren en funcionamiento antes de la puesta en marcha de este Registro (artículo 7 del Real Decreto-Ley).

De entre los actos inscribibles destaca en primer lugar la existencia del prestador y la actividad certificadora a desarrollar, así como la posibilidad o no de ejercer la actividad certificadora dentro de un sistema voluntario de acreditación. Además será objeto de inscripción la facultad del PSC de expedir certificados reconocidos.

Los datos, continuamente actualizados, que se reflejen en este Registro público podrán ser consultados tanto por la vía tradicional de certificaciones registrales como por vía telemática.

En el RDL 14/1999, la principal norma estatal que regula la firma electrónica y la situación de los PSC, no profundiza en el funcionamiento del Registro de PSC, y deja abierta la puerta a un posterior desarrollo por vía reglamentaria que todavía no ha tenido reflejo en el ordenamiento jurídico español.

Por último, no conviene confundir la acreditación con el registro de PSC. La diferencia se comentará posteriormente, simplemente citar que el artículo 2 letra ll dice que por acreditación voluntaria del prestador de

servicios de certificación se entenderá la "resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión".

2.5 Obligaciones legales

El Real Decreto-Ley 14/1999, de 17 de septiembre, establece una serie de obligaciones, de carácter general, que cualquier PSC deberá cumplir y, además, unas obligaciones de carácter más específico que serán únicamente exigibles a aquellos PSC que expidan certificados reconocidos.

En relación con las obligaciones generales hay que señalar que, ante todo, el PSC deberá inscribirse en el Registro, como se ha comentado anteriormente. Esta primera obligación tiene su origen en el artículo 3.3 de la Directiva1 1999\93 del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica, cuando se establece la obligación de los Estados de establecer algún sistema que posibilite la supervisión de los PSC que expiden certificados

En segundo lugar, como obligación cuasi general (puesto que exceptúa un solo caso concreto), los PSC habrán de constatar, bien por sí mismos bien a través de persona que les represente y actúe por nombre y cuenta del prestador, la identidad y demás circunstancias relevantes de la persona que solicite el certificado siempre que sean importantes para la utilización propia de los certificados.

Tendrán los prestadores de servicios, en virtud del artículo 11 apartado b), que poner a disposición del signatario los instrumentos necesarios para poder aplicar los datos de creación de firma, así como los instrumentos que sirvan para aplicar los datos de verificación de firma.

En cuarto lugar, por impacto de la normativa de protección de los consumidores y usuarios, se impone a los PSC ciertos deberes de información previa; en concreto, deben éstos informar a sus potenciales clientes, siempre antes de proceder a la emisión del certificado concreto, sobre el precio de los servicios, así como de las condiciones de uso del mismo, incluyendo limitaciones a su utilización y el régimen de responsabilidad del usuario.

Otra de las obligaciones impuestas a todos los PSC es la de que posean un registro de certificados, donde figuren todos los certificados emitidos, así como las circunstancias que afecten a una eventual pérdida de vigencia (por ejemplo suspensión, revocación, etc.) o que únicamente personas autorizadas puedan consultarlos, si los certificados únicamente están disponibles para verificación de firmas electrónicas. Lo que no se contempla en la regulación española es la posibilidad de solicitar por vía tradicional esta información relativa a la situación de los certificados, aspecto donde el Real Decreto-Ley resulta criticable, por haber alterado, en la "transposición" el sentido del texto europeo.

En efecto, la Propuesta de Directiva se preocupa porque se asegure que un certificado sólo se publique cuando exista consentimiento por parte del suscriptor. Por el contrario, el texto del Real Decreto-Ley exige que accedan personas autorizadas, algo que únicamente puede hacerse conociendo quién accede a cada certificado. La regulación europea no exige este control de acceso, por lo que debería modificarse en ocasiones futuras.

Una última obligación, de carácter negativo, hace referencia a la prohibición al PSC de almacenar o copiar las claves criptográficas privadas utilizadas para la creación de la firma electrónica de la persona a la que han prestado servicio, siempre que ésta no hubiere solicitado la prestación de este servicio.

En el supuesto de que el PSC cesase su actividad por el motivo que fuere, deberá comunicárselo con una antelación mínima de dos meses a los titulares de los certificados que hubiera expedido. Estos, a su vez, podrán optar por una de las siguientes opciones: que se deje sin efecto el certificado o que se transfiera a otro PSC en la fecha en que se produzca el cese efectivo del prestador. En los casos de cese, el PSC deberá comunicarlo, además de a los titulares, al Registro de Prestadores de Servicios de Certificación con una antelación mí-

nima también de dos meses y en los casos de la apertura de algún procedimiento concursal, en el momento en que tuviere conocimiento del mismo.

Una vez conocidas las obligaciones generales, se debe proceder a un análisis de aquellas obligaciones que, junto con las anteriores, deben cumplir todos los PSC que vayan a expedir certificados reconocidos.

La primera de estas obligaciones específicas es la de señalar el momento (fecha y hora) en el que un certificado se emite o se deja sin efecto.

Una segunda obligación que impone el Real Decreto es la de "demostrar la fiabilidad necesaria de sus servicios". Existen diversas posibilidades de cumplimiento de esta obligación: en primer lugar, el sistema de calidad y seguridad industrial, establecido por el Real Decreto 2200/1995, de 28 de diciembre, que desarrolla la Ley 21/1992, de 16 de julio, de Industria, permite prestar el servicio en condiciones de calidad similares a las que existen en otros sectores económicos, sistema que permite una autorregulación del mercado, por expulsión de los prestadores que no ofrecen garantías reales de calidad; en segundo lugar, el régimen que establece el Real Decreto-Ley, de acreditación voluntaria, basado en un sistema de evaluación previa independiente más el otorgamiento de una acreditación oficial, garantizando el cumplimiento de los requisitos que en cada caso se han establecido.

En ambos casos, el organismo nacional de acreditación (ENAC) y el organismo nacional de normalización (AENOR), trabajan con los organismos comunitarios de normalización (CEN - Comité Europeo de Normalización; Cenelec - Comité Europeo de Normalización Electrotécnica y ETSI - Instituto Europeo de Normas de Telecomunicaciones), en la definición de los regalmentos técnicos necesarios para el establecimiento de los citados sistemas de calidad.

Finalmente, decir que este segundo sistema será operado por el organismo público encargado de la supervisión de los prestadores; esto es, la Secretaría General de Comunicaciones de Ministerio de Fomento.

Algo similar ocurre con la obligación de demostrar la rapidez y la seguridad en la prestación del servicio.

Otra de las obligaciones impuestas a los PSC que emitan certificados reconocidos es la de contar con personal cualificado para el trabajo a desarrollar. Tal vez sea superflua esta obligación, puesto que al tratarse de un trabajo con características muy específicas, se hace necesario contar con personas cualificadas. En cualquier caso, conviene tener en cuenta que el mero hecho de cumplir con esta obligación no exime a la empresa de responsabilidad por una actuación culposa del personal a su servicio.

En el apartado e) del artículo 12, el legislador vuelve a hacer referencia a la fiabilidad de los productos a utilizar, mostrándose totalmente impreciso, aunque sí hay que decir que esta fiabilidad tiene como razón de ser la obligación que se impone al PSC de garantizar la seguridad técnica y criptográfica del proceso de certificación.

El PSC habrá de garantizar a sus clientes la confidencialidad de los datos de creación de firma durante el proceso de generación del certificado. A pesar de que esta es una obligación que solamente se impone a los PSC que emitan certificados reconocidos, podría pensarse que tal vez hubiera debido ser una obligación a imponer a todos los PSC.

Otra obligación especial, que según algunos debería de ser aplicable a todas las entidades certificadoras es la de poseer un seguro de responsabilidad por los daños y perjuicios causados a los usuarios de los servicios y a los terceros perjudicados. El Real Decreto 14/1999 da la opción al PSC de optar por un contrato de fianza mercantil (suscrito con una entidad crediticia) o por un seguro de caución, de tal manera que tengan los recursos económicos necesarios para poder afrontar un eventual riesgo. Esta garantía será como mínimo de un 4% del importe límite total de las transacciones en las que se pueda hacer uso de todos los certificados emitidos por la entidad certificadora, con un mínimo de mil millones de pesetas.

Esta obligación de aseguramiento tal vez pueda considerarse demasiado gravosa para los PSC, puesto que

la garantía a constituir solamente pueden asemejarse a los seguros que suscriben las compañías aéreas. Por otra parte, existen dudas acerca de la oportunidad de establecer un seguro de caución, habida cuenta de que lo que se asegura no es la insolvencia del prestador, sino su responsabilidad profesional. En cualquier caso, de establecerse un límite de endeudamiento del suscriptor del certificado, podría aceptarse la calificación del seguro como de crédito, pero nunca de caución.

En relación con el almacenamiento de información sobre certificados, existen unas obligaciones específicas para los PSC que emitan certificados reconocidos: en primer lugar, la de mantener registrada la documentación e información relativa a los certificados reconocidos emitidos durante un período de tiempo de quince años y en segundo lugar, utilizar sistemas lo suficientemente seguros de almacenaje de certificados, de tal modo que, según expresa el artículo 12 j):

1. Sólo personas autorizadas puedan consultarlos, si éstos únicamente están disponibles para verificación de firmas electrónicas, dicción legal que hemos criticado anteriormente.

2. Únicamente personas autorizadas puedan hacer en ellos anotaciones y modificaciones, donde "ellos" se refiere a los registro, nunca a los certificados, que, como todo el mundo sabe, son inmodificables.

3. Pueda comprobarse la autenticidad de la información, en el sentido de información garantiza por el prestador, mientras el certificado se encuentre en vigor y el registro donde se contiene el certificado que se consulta es también "auténtico".

4. El signatario o la persona autorizada para acceder a los certificados, pueda detectar todos los cambio técnicos que afecten a los requisitos de seguridad mencionados.

Como se ha podido apreciar, en un primer acercamiento a las obligaciones impuestas a los PSC, podemos extraer como conclusiones que:

1. El legislador se ha mostrado impreciso y poco claro en alguna de las obligaciones.

2. El aseguramiento de las PSC resulta ser demasiado gravoso

3. La mayoría de las obligaciones específicas debieran pasar a ser consideradas como obligaciones generales dada su importancia para los suscriptores de certificados

4. De hecho, la prestación de un servicio de certificación donde el certificado no se encuentre reconocido, donde el prestador no se halle acreditado, y donde el dispositivo seguro de creación de firma no haya recibido el preceptivo certificado de aceptación, tiene poco valor en el mercado.

2.6 Sistemas voluntarios de acreditación

Con la finalidad de mantener un alto nivel de la calidad de los servicios de certificación y de proteger los derechos de los usuarios de certificados, se crean, en virtud del artículo 6 del RDL 14/1999 los denominados "sistemas voluntarios de acreditación de los prestadores de servicios de certificación de firma electrónica". Esto no es más que un sistema de evaluación que finaliza con una resolución en la cual se establece bien una acreditación o bien una certificación. Se trata, pues, de un procedimiento totalmente voluntario y totalmente compatible con la libre constitución de PSC.

Aporta este sistema una serie de efectos positivos muy a tener en cuenta, tanto por los PSC como por los propios usuarios de productos de firma electrónica. Así, a título ejemplificativo, en relación con los efectos jurídicos de la firma (art. 3.1 párr. 2º) 2, puede decirse que se sitúan en una posición más ventajosa aquéllas fir-

mas basadas en certificados reconocidos que se hubieren expedido por un PSC acreditado.

Sometiéndose a este sistema de evaluación, se puede optar por conseguir la acreditación de la actividad certificadora, o bien, por la "certificación del producto de firma electrónica que empleen" los PSC (según versa el artículo 6 apartado 3º).

A efectos de este sistema, actuarán como organismos de evaluación entidades acreditadas a las que se les hubiera atribuido esta facultad por parte de una entidad independiente. Este tema, así como el relativo a las normas que habrán de regular el proceso de evaluación se dejan postergados hasta que un Real Decreto desarrolle estos temas. De esta manera, en tanto no se apruebe esta normativa en desarrollo del artículo 6, no se podrá acreditar ningún prestador de servicios de certificación, ni proceder a la certificación de productos de firma electrónica; y, por lo tanto, nadie se podrá beneficiar de los efectos positivos que produce este sistema voluntario de evaluación.

El legislador, a diferencia de lo anteriormente comentado, sí deja claro que la evaluación no es gratuita, sino que está sujeta al pago de una tasa (a la que se hace mención en el artículo 23 c del RDL). Esta tasa, que se podrá actualizar por la vía de Real Decreto, asciende a 285,48 euros (47.500 ptas.); sin embargo no se especifica modo alguno para liquidarla, sino que se envía a desarrollo reglamentario posterior.

2.7 Responsabilidad de los prestadores

La actividad que desarrollan los PSC genera una serie de relaciones, tanto de naturaleza contractual como extracontractual (con el titular del certificado y el usuario, principalmente), que plantean la necesidad de clarificar, además de los derechos y obligaciones inherentes a la relación, la eventual responsabilidad en que incurre cada uno de los sujetos.

En el caso concreto de los prestadores de servicios de certificación, éstos no pueden conocer todas y cada una de las operaciones que se ejecuten con los certificados emitidos, ni siquiera autorizar individualmente cada operación, por lo que no resultaría sencillo "fijar un límite de responsabilidad por remisión al importe de la operación u operaciones para las cuales se hubiera utilizado un certificado"3.

Dada la importancia de este tema, el Real Decreto-Ley español dedica el artículo 14 a establecer el régimen de responsabilidad de los PSC.

El legislador español sigue los criterios de responsabilidad que se establecen en la Propuesta de Directiva sobre firma electrónica. De hecho, se pueden establecer algunos paralelismos entre el artículo 14.1 del Real Decreto con el 6.1 de la Directiva 1999\93, y del 14.2 con el artículo 6.3 comunitario.

Así, el supuesto general será el de la existencia de responsabilidad del PSC por los daños y perjuicios causados (dentro del ámbito del ejercicio de la actividad que desarrollan) "a cualquier persona". El legislador, pues, no especifica frente a quiénes puede responder el prestador de servicios; de esta manera podrán ser tanto el titular del certificado como terceros usuarios e, incluso, terceros no usuarios pero sí perjudicados (en cualquier caso, habría que analizar si en el caso concreto nos encontramos ante responsabilidad contractual o extracontractual).

Parece que, en principio, el legislador español opta por un tipo de responsabilidad que pudiera parecer objetiva (responderán los PSC por los daños y perjuicios que causen cuando incumplan las obligaciones legalmente estipuladas); sin embargo al final resulta tener carácter eminentemente subjetivo, al hacer referencia a la posibilidad de que el PSC incurra en un comportamiento negligente.

En este caso, sucede que el prestador de servicios de certificación puede limitar su responsabilidad frente a todas las partes, exigiendo que adhesión al convenio de verificación de firmas electrónicas y certificados di-

gitales de aquellas personas (terceros que confían en certificados) que han de resultar usuarios de los mismos. De esta forma, por vía contractual, se evitar la responsabilidad universal. Es condición indispensable para implantar esta solución indicar debidamente en el certificado esta situación, dentro del campo de límites de uso, que se encuentra previsto en el Real Decreto-Ley.

En la normativa española se dice que "en todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia". En este punto es importante señalar que se está estableciendo una presunción de culpa para el PSC, de la que solamente se liberará mediante la aportación de una prueba a su favor (estamos, pues, ante una "inversión de la carga de la prueba").

La prueba es, pues, una carga para el PSC que, además de actuar diligentemente deberá probar dicho comportamiento. Esto tiene su razón de ser, y es que resulta más sencillo que el PSC demuestre que actuó correctamente que el perjudicado tenga fácil acceso a medios que puedan demostrar que el PSC realizó actos que le provocaron un daño debido a conductas culposas o dolosas.

En cualquier caso, tal y como está redactado el Real Decreto-Ley español, se pueden suscitar dudas de carácter interpretativo, en el sentido de que no queda claro si el incumplimiento de las obligaciones legalmente estipuladas, independientemente de si ha existido o no diligencia por parte del PSC, provoca incurrir en responsabilidad por los daños y perjuicios que se causen.

Un supuesto de carácter más específico se detalla en el artículo 14 párrafo 2º, que hace referencia a la responsabilidad en que incurren los PSC por los daños y perjuicios causados por un uso de los certificados reconocidos diferente al que se hubiera establecido en el momento de la emisión del mismo.

El prestador de servicios, según lo establecido en la normativa española tendrá que afrontar la indemnización que le corresponda por haber incurrido en responsabilidad en primer lugar con la garantía que tuviere constituida, y, en caso necesario, deberá seguirse el principio de responsabilidad universal consagrado en el artículo 1911 del Código Civil español, en el que se hace referencia a que se responderá de la deuda contraída con todos los bienes presentes y futuros del deudor.

2.8 Supervisión y control

El cumplimiento de las obligaciones legalmente establecidas a los prestadores de servicios de certificación será controlado por la Secretaría General de Comunicaciones, dependiente del Ministerio de Fomento. Esta Secretaría actúa de oficio, siempre que medie una petición razonada al respecto proveniente tanto del Ministerio de Justicia (recordar que el Registro de Prestadores de Servicios de Certificación depende de este Ministerio) como de cualquier otro órgano o ente administrativo o de cualquier persona (física o jurídica) con interés en este particular.

En la actividad inspectora, los PSC tienen la obligación (además de las ya comentadas) de facilitar información y medios para el ejercicio de la actividad de supervisión, así como consulta de documentos y acceso a las instalaciones. Este deber de colaboración se entiende que es con la Secretaría General de Comunicaciones y con los agentes o personal inspector.

En los supuestos en los que, mediante una actividad inspectora, se detectase la existencia de una violación de la normativa, la Secretaría General de Comunicaciones tiene la facultad de ordenar a los PSC la adopción de las medidas apropiadas para que cumplan las exigencias establecidas en el Real-Decreto y demás disposiciones legales. Sin embargo, si la infracción versase sobre tratamiento de datos, podrá iniciarse, a través de la Agencia de Protección de Datos, un procedimiento sancionador contra el PSC.

2.9 Régimen sancionador

El legislador español en el artículo 25 del RDL 14/1999, opta por diferenciar tres tipos de infracciones: leves, graves y muy graves. De entre las primeras pueden destacarse: la expedición de certificados reconocidos que no cumplan con los requisitos previstos en la normativa y la de no facilitar información a la autoridad competente en casos de inspección llevados a cabo por la Secretaría General de Comunicaciones.

La diferencia principal entre las infracciones graves y las muy graves es la producción efectiva del daño y la característica de si el PSC emite o no certificados reconocidos. Así, según el tipo de infracción en el que se haya incurrido, procederá una u otra sanción.

El órgano que ejerce esta potestad sancionadora es la Secretaría General de Comunicaciones, que podrá, además, adoptar cuantas medidas cautelares estime convenientes en cada uno de los casos, siempre con arreglo a lo dispuesto en el ordenamiento común, y que podrán consistir en: cese temporal de la actividad de certificación, suspensión de la vigencia de los certificados emitidos por el PSC, ...

A diferencia de las medidas cautelares, las sanciones a imponer tienen, por regla general, carácter pecuniario, pero conviene tener en cuenta dos salvedades:

En los casos en los que el PSC, en el plazo de cinco años cometa dos o más infracciones de las consideradas muy graves, podrá imponérsele la sanción consistente en prohibir que actúe en España durante un plazo máximo de dos años.

Las sanciones impuestas, siempre que sean por motivo de infracción grave o muy grave, se anotarán en el Registro de Prestadores de Servicios de Certificación, procediendo a su cancelación registral cuando hubiere transcurrido el plazo de prescripción.

Todas las sanciones las impondrá la llamada "comisión de infracciones". A la hora de proceder a la imposición de las multas, se deberán tener en cuenta varios factores además de la gravedad de la infracción:

1. La repercusión social de la infracción.

2. El daño causado, si no se ha tenido en cuenta para calificar la infracción como leve, grave o muy grave.

3. El beneficio que hubiera reportado al sujeto infractor la comisión del ilícito.

Por último, y a título meramente ejemplificativo, cabe decir que la máxima sanción pecuniaria que cabe imponer tras una infracción leve es la de 2.000.000 de pesetas, por una infracción grave, 50.000.000 de pesetas, y por una infracción muy grave, 100.000.000 ptas.

1 Art. 3.3: "Los Estados miembros velarán por que se establezca un sistema adecuado que permita la supervisión de los proveedores de servicios de certificación establecidos en su territorio que expiden al público certificados reconocidos". DOCE, de 19 de enero de 2000 (L13)"FIRMA DIGITAL Y ENTIDADES CERTIFICADORAS. REGULACIÓN LEGAL EN CHILE"

Firma Digital y Proveedores de Servicios de Certificación.

Renato Javier Jijena Leiva (Chile)
Abogado
Profesor de Derecho Informático UGM
Diplomado en Derecho Informático - Universidad de Zaragoza / Chile
renatojijena@entelchile.net
rjijena@ucv.cl

I. FIRMA DIGITAL Y PROVEEDORES DE SERVICIOS DE CERTIFICACION.

Tratándose de comercio electrónico, la firma digital es el sustituto tecnológico de la firma manuscrita u "ológrafa", y quien la use, junto con acreditar fehacientemente su identidad y con la imposibilidad de posteriormente repudiar el envío de un mensaje, jurídicamente hablando está manifestando su voluntad en orden a realizar una determinada transacción electrónica con un también determinado "co-contratante". Con una gran diferencia: ...la firma digital es mucho más segura.

En consideración al principio jurídico del necesario resguardo de la "Fe Pública"[1] y para mantener el "Orden Público Económico" y la "Buena Fe" involucrados en las transacciones electrónicas, tecnológica y legalmente han surgido las denominadas "Autoridades Certificadoras" o, dicho más adecuadamente, los "Proveedores de Servicios de Certificación" de firmas digitales[2].

Junto con las medidas técnicas de resguardo y certeza provistas por la criptografía para disponer de un entorno seguro en relación con la autenticación electrónica, y porque las firmas digitales van más allá que la mera encriptación que sólo asegura la confidencialidad de un documento, jurídicamente se ha regulado la existencia de entidades que certifiquen -generando los bits necesarios para hacerlo- y publiciten las firmas digitales que se usen[3] o, dicho de otro modo, que en un proceso de validación autentifiquen la identidad de los emisores y receptores que envían o reciben los mensajes firmados, cuyos antecedentes personales o nominativos además registran o archivan. Así, al lograrse que el receptor de un mensaje sepa indubitadamente que el emisor del mismo es realmente quien dice ser y que éste, a su vez, posteriormente no pueda negar el envío, se alcanzan mayores grados de confianza en las relaciones comerciales electrónicas o virtuales.

La trascendencia pública de su función pasa por el hecho de que cuando certifican dígitos o algoritmos y la pertenencia de esos dígitos a personas concretas y determinadas por sus características propias, están ejerciendo la potestad jurídica de otorgar "Fe Pública" en el marco de las transacciones comerciales.

Naturaleza (sobre todo jurídica) de los Proveedores de Servicios de Certificación Electrónica.

Desde un punto de vista tecnológico, no cualquiera puede o está capacitado para ofrecer el uso de firmas digitales y de mecanismos de encriptación. No se le puede encomendar la función de certificar tecnológica-

---

[1] Parafraseando al jurista uruguayo Eduardo Couture, la Fe Pública es una calidad particular de ciertos instrumentos que consiste -o depende- no sólo en la autoridada moral y técnica de quien los ha elaborado sino también en una ficción legal de que lo aseverado por una entidad facultada para hacerlo es verdad.

[2] El tema de la certificación de firmas digitales puede -y debe- ser analizado desde una perspectiva económica, ya que por cada firma digital certificada habrá que pagar una tarifa al proveedor del servicio. No es el ámbito, por cierto, de esta minuta.

[3] Así por ejemplo, si se está utilizando un sistema de criptografía "asíncrona" o de algoritmos "asimétricos", que contempla la operatoria de una pareja de dos claves o llaves únicas y correspondientes entre si, una pública y otra privada, de manera tal que ambas se corresponden -valga la redundancia- entre si de manera exclusiva y excluyente, el Proveedor de Servicios de Certificación deberá administrar un sistema de publicidad de las llaves en conformidad a la ley.

mente a personas naturales o a pequeños proveedores de hardware o software, ajenos a las realidades y a los procedimientos técnicos de quienes intervienen en el comercio electrónico. Sería un gran error encomendar el trabajo de otorgar llaves o firmas digitales y de registrar los antecedentes personales de aquellos a quienes se refieran a entidades o funcionarios auxiliares de la administración de justicia -como los notarios-, que apenas manejan procesadores de textos o programas de bases de datos o de informática registral.

También es definitivamente inviable centralizar la función de certificar en una única institución o entidad (sistema "cerrado"), como por ejemplo un sólo órgano estatal, un sólo ente empresarial o gremial, sólo el Colegio de Notarios de Chile.

Desde la perspectiva del derecho, se requiere que una ley establezca expresamente quienes son las entidades -personas jurídicas y/o naturales- que, además de estar capacitadas tecnológicamente para prestar servicios de firma digital, por cumplir con determinados requisitos legales y reglamentarios estarán dotadas de la potestad de otorgar "Fe Pública" respecto a que, en una fecha y hora determinada, personas perfectamente individualizadas realizaron o acordaron una operación de comercio electrónico en también determinados términos, antecedentes que posteriormente no podrán ser negados o "repudiados".

Esta normativa legal y reglamentaria además deberá contemplar las hipótesis de revocación, las causales de extinción y los casos de eventual cancelación de firmas o certificados digitales; establecer derechos y obligaciones o deberes -con las consiguientes responsabilidades- para las entidades que cumplan funciones de Proveedores de Servicios de Certificación[4]. Esta misma normativa deberá determinar las tarifas que se cobrarán por la generación, publicidad y archivo de las llaves o firmas, los sistemas operativos a utilizar, los posibles mecanismos de seguridad a aplicar[5] -con el cuidado de no vulnerar el principio de la "neutralidad tecnológica", etc.

El Organismo Acreditador o Licenciante de Entidades Certificadoras.

Es necesario dar un paso más en la cadena y llegar al primer nivel de la misma. Porque las personas jurídicas que presten servicios de Entidades Certificadoras a su vez también deben ser certificadas, o dicho de otra forma, porque la infraestructura de firma digital o el sistema que la regule tiene que posibilitar que también las llaves públicas de dichas Entidades Certificadoras -"de segundo nivel"-puedan ser conocidas de forma segura por los suscriptores o signatarios que requieran de sus servicios, de manera tal que ellos sepan fehacientemente que ha sido una Tercera Parte Confiable la que emitió un certificado válido y vigente, o dicho de otra forma, la que otorgó Fé Pública en el marco de una operación de Comercio Electrónico[6].

La Ley y su correspondiente Reglamento de Ejecución deberán, por ende, considerar la existencia de un órgano público (y no privado) competente técnicamente u "Órgano Acreditador o Licenciante de Certificadores" -el que en teoría o doctrina debería crearse-, que "a priori" fiscalice el cumplimiento de los requisitos que ella establece para la prestación de servicios de certificación (v.gr. programa de seguridad digital utilizado, sistemas de generación, archivo y administración de firmas digitales, etc.), autorizando el funcionamiento u otorgándole a la Entidad Certificadora una licencia y, desde un punto de vista tecnológico, emitiendo las llaves públicas de las Entidades Certificadoras y sus correspondientes certificados a efectos de validarlas. "A posteriori", esta autoridad velará porque se mantengan dichos requisitos establecidos para que una persona jurídica actúe como Entidad Certificadora.

---

[4] V.gr., determinar cuáles serán los horarios durante los cuales deberán mantenerse disponible el servicio de validación o certificación, o si deberá ser ininterrumpido; establecer un plazo obligatorio para el archivo o registro de las claves o llaves; etc.

[5] V.gr. SSL, SET, etc.

[6] En un informe evacuado por la ACTI en Julio de 1999, se distingue entre la "Entidad Certificadora de Primer Nivel" -que sería este organismo acreditador de certificadores o certificador raíz, proponiéndose al Ministerio de Economía al efecto- y las "Entidades Certificadoras de Segundo Nivel" -que serían las que hemos descrito más arriba y que operarían en el ámbito de las transacciones de Comercio Electrónico.

II. DECRETO SUPREMO N°81, DE JUNIO DE 1999, REGULADOR DEL USO DE FIRMAS DIGITALES Y DOCUMENTOS ELECTRONICOS AL INTERIOR DE LA ADMINISTRACION DEL ESTADO.

El Decreto aludido obedece a uno de los compromisos adoptados por una Comisión Presidencial de Nuevas Tecnologías que sesionó durante 1998, en orden a dotar a los órganos estatales del marco legal que permita el uso de la informática y de las telecomunicaciones en reemplazo de sus procedimientos manuales, específicamente en lo relacionado con el uso de firmas y de documentos digitales o electrónicos, pero sólo al interior de la Administración del Estado y no en las relaciones con los administrados. Así lo consigna, por cierto, el Considerando 3º del Decreto.

A. Comentarios a los fundamentos o considerandos.

El Considerando 4°, en su primera parte, establece acertadamente que los documentos "escritos" (debió decir "soportados magnéticamente") en soportes informáticos no se diferencian en esencia de los escritos en soportes tradicionales como el papel, y que en la actualidad existen tecnologías que generan firmas digitales sobre la base de conjuntos de claves que aseguran inequívocamente la autoría e integridad de un documento electrónico, mejor aún o con más seguridad que cuando la firma es ológrafa o soportada en papel.

B. Comentarios al articulado.

1) Desde el punto de vista de la técnica legislativa, los tan sólo 10 artículos que conforman el Decreto se agrupan en tres Títulos, sobre "Disposiciones Generales" el primero, acerca "Del Documento Electrónico" el segundo, y sobre la "Regulación de la Firma Digital" el tercero.

2) El Título I lo conforman sólo tres artículos. El artículo 1° señala el objeto del Decreto, el 2° formula algunas definiciones y el 3° contiene una declaración de principios.

El artículo 1° señala el objeto de la norma, a saber, la regulación de la utilización de la firma digital y los documentos electrónicos "como soporte alternativo" -es una opción para los entes estatales- a la instrumentalización en papel de sus actuaciones. Agrega el artículo que el Decreto establece además las condiciones en que los datos contenidos en un soporte electrónico se considerarán emanados de una persona determinada.

El inciso segundo del artículo 1º delimita el ámbito de aplicación, esto es, los órganos estatales mencionados en el artículo 1º de la Ley Orgánica Constitucional de Bases, salvo la Contraloría General de la República, el Banco Central y las Municipalidades, los que, empero, pueden acogerse voluntariamente al Decreto enviando al efecto una comunicación por escrito a la SEGPRES.

El artículo 2° define los conceptos de "documento electrónico"[7], "firma electrónica"[8], "firma digital"[9], "clave privada"[10], "clave pública"[11] (los tres íntimamente ligados), "integridad"[12] y "certificado de firma digital"[13]. Claramente queda establecido -aunque no se dice- que se optó por un sistema de algoritmos asimétricos o de criptografía de dos llaves.

---

[7] "Toda representación informática que da testimonio de un hecho".

[8] "Código Informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su transmisor desconocer la autoría del mensaje en forma posterior".

[9] "Especie de firma electrónica que resulta de un proceso informático validado, implementado a través de un sistema criptográfico de claves públicas y privadas".

[10] "Es aquella que sólo es conocida por el titular del par de claves y que es usada para añadir una firma digital a un documento electrónico, o para desencriptar un documento electrónico previamente encriptado por medio de la correspondiente clave pública".

[11] "La que registra en el sistema el ministro de fe del servicio respectivo y que es empleada para verificar la firma digital añadida a un documento electrónico por el titular, o para encriptar documentos destinados a ser transmitidos a él".

[12] "Cualidad de un documento electrónico que consiste en no carecer de ninguna de sus partes ni haber sido alterado después de su firma".

[13] "Documento electrónico emitido por el ministro de fe del servicio respectivo que acredita la correspondencia entre una clave pública y la persona que es titular de la misma".

El artículo 3°, a manera de declaración de principios, establece que para utilizar soportes, medios y aplicaciones electrónicas, informáticas y telemáticas en las actuaciones administrativas deberán adoptarse las medidas técnicas y administrativas -"o de organización" dice la norma- que sean necesarias para garantizar las propiedades de las firmas digitales; éstas propiedades son la autenticidad de las partes, la integridad o conservación de la información, y la no repudiación de un mensaje.

3) El Título II comprende los artículos 4°, 5° y 6° para aludir al documento electrónico, para ser más precisos, al documento electrónico que es firmado digitalmente.

El artículo 4º sienta los principios de una total homologación entre los documentos soportados en papel y los soportados magnéticamente. Primero señala que los documentos de los órganos señalados en el artículo 1º escritos en soporte electrónico producirán los mismos efectos que los escritos en soporte papel; y luego establece que en dichos documentos la firma digital sustituirá a la firma ológrafa del funcionario que lo emite y producirá los mismos efectos que aquella.

La segunda parte del inciso segundo establece una consecuencia lógica: cuando un documento electrónico sea firmado digitalmente se entenderá que emana del funcionario titular de dicha firma digital, y producirá los mismos efectos jurídicos que el documento escrito y firmado manualmente y soportado en papel.

Los artículos 5º y 6º son en nuestra opinión un gran aporte, toda vez que al abordarse el tema de la impresión en papel de los documentos electrónicos se definen claramente como "originales" los soportados magnéticamente y como "copias" las impresiones, exigiendo siempre la debida "certificación" manual o electrónica.

El artículo 5º -preocupado del tema de la relación con los ciudadanos- establece que los documentos electrónicos firmados digitalmente y que deban ser publicados o notificados a un particular, deberán ser "traspasados a soporte de papel", y su correspondencia con "el original electrónico" será certificada -obvio que manualmente- por el respectivo ministro de fe de cada Servicio. El inciso segundo pero del artículo 6º, agrega que la impresión en papel de un documento electrónico firmado digitalmente se entenderá copia autorizada del mismo, siempre que el ministro de fe del servicio acredite su correspondencia con el electrónico mediante su firma ológrafa y en conformidad a las reglas generales.

El inciso primero del artículo 6º se plantea desde la perspectiva contraria y exige certificación "electrónica", esto es, de lo que ocurre cuando se "escanean" (de "scanner") documentos soportados en papel. Establece la norma que para todos los documentos regidos por el Decreto las copias informáticas de documentos originalmente producidos en papel "o en otro medio no electrónico" (¿?) se entenderán copias autorizadas, con la condición que el ministro de fe del servicio respectivo acredite su correspondencia con éste mediante su firma digital debidamente certificada.

4) El Título III alude a la "Regulación de la Firma Digital" en cuatro artículos. Más específicamente, aborda los procedimientos que deben realizarse para generarla o elaborarla, para verificarla o validarla y para certificarla o establecer un vínculo entre una persona determinada y un sistema de validación.

Los artículos 7º y 8º establecen que las firmas digitales se generarán a través de un sistema criptográfico que constará de un par de claves correlativas, una privada y otra pública. Es errado en parte y quizás podría aclararse -desde un punto de vista tecnológico- el inciso que señala que "la clave privada del emisor asegurará la autoría e integridad del documento electrónico que se envía mientras que la pública del receptor asegura la encriptación del mismo" y que "mediante la clave pública del emisor del documento se verificará lo anterior y podrá desencriptarse el documento". Ocurre que para "encriptar" un mensaje un emisor puede utilizar la llave pública del eventual receptor o destinatario, y para "desencriptar" es necesario usar la llave privada de ese mismo receptor.

El artículo 9º es el resultado de haberse descartado la opción de legislar en materia de Entidades Certifi-

cadoras al interior de la Administración Estatal. En síntesis, lo más importante es que se establece que el ministro de fe mantendrá una nómina actualizada de las claves públicas de los funcionarios del servicio respectivo que tengan una firma digital, cuya clave pública se acreditará mediante un certificado de firma digital, misma que podrá ser suspendida (cuando un funcionario no ejerza temporalmente sus funciones) o revocada (cuando un funcionario cese en sus funciones).

III. ANALISIS DEL BOLETIN Nº2348-07, UN "PROYECTO DE LEY SOBRE DOCUMENTOS ELECTRONICOS".

A. Observaciones a los fundamentos contenidos en la presentación de la MOCIÓN.

1) Razones invocadas para justificar la brevedad de la MOCIÓN.

Es errado afirmar que el Derecho Comparado se ha caracterizado por dictar normas breves y simples al regular el uso de firmas y de documentos digitales o electrónicos, intentando justificar la brevedad de la MOCIÓN (sólo 7 artículos) y el haberse optado por un proyecto simple, "de fácil comprensión" (cuando en estricto rigor la brevedad lo hace inaplicable e ininteligible) y de objetivos limitados.

No es procedente afirmar que la Directiva de la Unión Europea de 1998 es un modelo a imitar por su brevedad, sin darse cuenta que sólo se trata de un texto marco que contiene principios mínimos o esenciales, y que reenvía a las legislaciones de cada Estado miembro el desarrollo acabado de los temas. Ni Alemania, ni Argentina, ni Italia, países a los cuales se alude, han optado por proyectos "tan simples o generales" como el contenido en la MOCIÓN.

La MOCIÓN llega al extremo de proponer un texto legal tan breve que deja de lado aspectos esenciales a toda ley sobre firmas digitales, tales como las condiciones en que éstas producirán efectos legales[14], la regulación de la naturaleza, requisitos, deberes y funciones de los Proveedores de Servicios de Certificación, y la estructura del régimen o sistema de acreditación[15], el cual, por cierto, incluso podría encomendarse en última instancia a un organismo certificador internacional[16].

2) Decisiones y recomendaciones erradas acerca de la naturaleza de los Proveedores de Servicios de Certificación.

No estamos de acuerdo y nos parece errado que en la presentación de la MOCIÓN se insista en sugerir, restrictivamente, que tratándose de las Entidades Certificadoras el rol podrían asumirlo los actuales notarios públicos de manera de aprovechar su prestigio (debieron decir sus facultades o potestad) como ministros de fe[17]. Los notarios no están preparados tecnológicamente, y su participación mediante la forma en que tradicionalmente han desempeñado y siguen haciéndolo su función sería un obstáculo y un freno al desarrollo del Comercio Electrónico, que, por lo demás, no haría sino encarecer los costos y dilatar el tiempo de las operaciones de las transacciones virtuales.

Del mismo modo, no es un argumento fundado el que se hayan reconocido a los notarios como ministros

14 Tenemos en mente el propuesto artículo 6º.

15 Desde la perspectiva de quienes cumplirán labores de "Entidades Certificadoras", de modo alguno nos parece que sus requisitos, atribuciones o funciones y sus responsabilidades deban ser encomendados a una norma reglamentaria. Por su importancia, se requiere que estos temas sean regulados con normas de mayor estabilidad como son las leyes propiamente tales.

16 Cabe investigar y reflexionar quizás, en lo que se ha hecho con las normas ISO 9000 y su cumplimiento y con los INCOTERMS en materia de comercio exterior, sobre todo pensando en el valor legal en Chile de los certificados obtenidos en el extranjero.

17 Si se lee con detenimiento el Preámbulo de la Directiva sobre Firma Digital del Consejo de Europa, fácilmente puede repararse en que ella consigna que la utilización de algoritmos asimétricos a la hora de estamparse firmas digitales requiere la necesidad de establecer un sistema de Proveedores de Servicios de Certificación suficiéntemente amplio y no restringido a la acción o a la participación certificadora de sólo los notarios públicos o escribanos.

de fe para la certificación de firmas electrónicas atendido el hecho de haberse ***"optado por un proyecto simple, de fácil comprensión y de objetivos limitados"*** que no modificara el ordenamiento jurídico existente, como señala la introducción del proyecto. La regulación legal de las Entidades Certificadoras, a diferencia de lo estimado por la MOCIÓN, es precisamente un nuevo tópico o una nueva materia que requiere de una también nueva regulación legal y reglamentaria, a pesar del arduo trabajo que esto demande.

B. Observaciones al articulado propuesto.

1). Articulado de la MOCIÓN.

Artículo 1º: Se entenderá por documento electrónico toda representación digital que de testimonio de un hecho.

Artículo 2º: Todos los actos jurídicos pueden celebrarse válidamente por medio de documentos electrónicos, salvo que la ley exija expresamente que sean escritos en un soporte papel o requiera la concurrencia personal de al menos una de las partes.

Artículo 3º: Los documentos escritos en un soporte electrónico producirán los mismos efectos que los escritos en un soporte de papel, lo que será especialmente aplicable en los siguientes casos: a) Cuando la ley exija que ciertos actos consten por escrito o prevea consecuencias jurídicas para su falta de escrituración; b) Cuando se presenten documentos electrónicos como prueba en juicios.

Artículo 4º: Los documentos electrónicos valdrán como instrumentos públicos o privados según las reglas generales. La firma electrónica sustituirá el uso de cualquier sello, timbre, visto bueno u otra marca distintiva que se requiriese para la validez del documento si este hubiere sido escrito sobre un soporte de papel.

Artículo 5º: Por firma electrónica debe entenderse el conjunto de dígitos o números que permiten determinar que el creador de la misma es quien efectivamente ha aprobado el contenido del documento firmado y que dicho contenido no ha sido modificado con posterioridad.

Artículo 6º: La firma electrónica que cumpla con los requisitos establecidos en el Reglamento tendrá los mismos efectos jurídicos que la firma ológrafa.

Artículo 7º: El reglamento de esta ley fijará las normas técnicas que deberán cumplirse para que una firma electrónica sea considerada válida, así como los protocolos y estándares de seguridad que se requieran para un adecuado funcionamiento del sistema certificatorio. Regulará, además, los requisitos de la firma electrónica y los mecanismos para certificarla, las limitaciones que tendrá el uso de la firma electrónica y toda otra cuestión que incida en la utilización de documentos electrónicos y firmas electrónicas y no sea materia de ley.

2) Título de la Moción.

Es parcial hablar de un "PROYECTO DE LEY SOBRE DOCUMENTOS ELECTRÓNICOS". Hay que agregar la referencia a las firmas digitales y al tema del valor probatorio de ambos. Recuérdese que la firma digital que se intenta regular en la MOCIÓN no es el único documento o hecho del mundo digital que puede necesitar ser acreditado legalmente en un proceso tramitado ante los Tribunales de Justicia. Nosotros proponemos el siguiente nuevo encabezado: "SOBRE LA FIRMA Y EL DOCUMENTO ELECTRÓNICO Y SU VALOR PROBATORIO".

3) Técnica jurídico-legislativa del proyecto.

Los tan sólo siete artículos carecen de una sistematización adecuada, por cuanto no tienen un orden lógico entre ellos en atención a su contenido y los temas que debieran regularse. Además de que no se dividen en Títulos, Párrafos, etc. Una sistematización lógica, contenida en el proyecto propuesto más adelante, podría ser la siguiente: Título Preliminar; Título Primero: De la firma digital o electrónica; Título Segundo: De los Pro-

veedores de Servicios de Certificación de llaves digitales o electrónicas; Título Tercero: De la Secretaría de Seguridad Electrónica (Organismo Licenciante); Título Cuarto: Del documento digital o electrónico; Título Quinto: Del valor probatorio de la firma y del documento digital o electrónico; etc.

4) Análisis de los artículos 1º y 2º.

El artículo 1º entiende por documento electrónico a "toda representación digital que dé testimonio de un hecho". Coincidente con la amplia definición[18] (al igual que lo hacen al menos las legislaciones sobre firma digital de Italia, Argentina y Singapur), el artículo 2º establece que por regla general todos los actos jurídicos podrán celebrarse válidamente por medios electrónicos -siempre, por cierto que se cumplan los requisitos legales y reglamentarios respectivos-.

5) Análisis de los artículos 3º y 4º.

Simplemente un comentario general: la opción de instar por una homologación total entre firmas manuscritas y digitales y entre documentos soportados en papel o digital o magnéticamente, recogida por ambos artículos con el objeto de evitar la existencia de regímenes jurídicos paralelos, nos parece adecuada, a pesar de ser revolucionaria, a pesar de ir contra un sistema jurídico como el chileno que en numerosas normas civiles y procesales constantemente alude a "documentos escritos", que "deberán constar por escrito", a "principios de prueba por escrito", etcétera.

6) Análisis del artículo 5º.

El artículo define lo que debe entenderse por firma electrónica. La definición es muy "engorrosa" o poco clara a pesar de que sigue la tendencia del Derecho Comparado en orden a referirse al contenido de la firma y su relación con la entidad certificadora[19], y al parecer subyace en ella la existencia de un mecanismo asimétrico de llaves, por el hecho de pedirse que la firma impida que el contenido de un mensaje sea modificado con posterioridad o, dicho técnicamente, "no repudiado". Hablar de "dígitos o números" nos lleva al ámbito del sistema binario y de la lógica formal-proposicional, a los caracteres "0 y 1" o a los valores "verdadero o falso". Nos parece más adecuado definir en consideración a los elementos y a los efectos jurídico-tecnológicos de la "PKI" o infraestructura de llave pública.

Debería retomarse el concepto que desde 1995 se ha incorporado a nuestras normas reglamentarias para el Comercio Electrónico transaccional, a saber, establecer que la firma electrónica es el sustituto digital de la firma manuscrita que en el marco del intercambio electrónico de datos permite al receptor de un mensaje electrónico verificar con certeza la identidad proclamada por el transmisor, impidiendo a éste último desconocer la autoría del mensaje en forma posterior.

7) Análisis del artículo 6º.

Es por decir lo menos peligrosa y ambigua una norma que señale que "la firma electrónica que cumpla con los requisitos establecidos en el Reglamento tendrá los mismos efectos jurídicos que la firma ológrafa".

El señalamiento de los requisitos estimamos que no es una cuestión técnica que pueda reenviarse por completo a la potestad reglamentaria subordinada o de ejecución, sino que debe ser materia de la norma legal. Mucho más adecuado, seguro y completo sería un artículo que, en consideración a la criptografía asimétrica o de dos llaves, afirmara que se presume que una firma digital o electrónica tiene el mismo efecto que una firma manuscrita u ológrafa, en la medida que ella sea verificada por referencia a una clave o llave pública incluida en un certificado válidamente emitido por un Proveedor de Servicios de Certificación debidamente licenciado.

8) Análisis del artículo 7º.

La norma consigna el reenvío en materia de normas técnicas que deberán cumplirse para que una firma electrónica sea considerada válida; los protocolos y estándares de seguridad que se requieran para un adecuado funcionamiento del sistema certificatorio; los requisitos de la firma electrónica y los mecanismos para certificarla, las limitaciones que tendrá el uso de la firma electrónica y toda otra cuestión que incida en la utilización de documentos electrónicos y firmas electrónicas y no sea materia de ley.

Constituye un grave error u omisión el reenviar a un reglamento la definición de las normas técnicas que deberán cumplirse para que una firma electrónica sea considerada válida, sin previamente señalar cuáles serán los requisitos legales para alcanzar el mismo objetivo. Por eso, insistimos en la crítica hecha al artículo 6°, a saber, que es esencial corregir el proyecto e introducir un artículo que establezca que se presumirá que una firma digital o electrónica tendrá el mismo efecto que una firma manuscrita u ológrafa, en la medida que ella sea verificada por referencia a una llave pública incluida en un certificado electrónico válidamente emitido por un Proveedor de Servicios de Certificación.

9) Otras materias faltantes.

Ya anticipamos que una norma "legal" sobre firmas y documentos digitales, magnéticos o electrónicos debe, necesariamente, además: contemplar los requisitos en virtud de los cuales una firma será considerada válida; referirse a las hipótesis de revocación, las causales de extinción y los casos de eventual cancelación de firmas o certificados digitales; determinar la naturaleza jurídica de quienes desempeñarán las funciones de Proveedores de Servicios de Certificación y establecer sus derechos y obligaciones o deberes -con las consiguientes responsabilidades-; ...todas cuestiones que no son de carácter técnico y no pueden encomendarse a la potestad reglamentaria subordinada o de ejecución.

"Sobre la no Protección de la Intimidad en Chile. Análisis de la Ley 19.628, de agosto de 1999"

Renato Javier Jijena Leiva (Chile)
Abogado
Profesor de Derecho Informático UGM
Diplomado en Derecho Informático - Universidad de Zaragoza - Chile
renatojijena@entelchile.net
rjijena@ucv.cl

I. INTRODUCCION.

Si bien es cierto el problema de la protección legal de datos personales frente al tratamiento computacional de los mismos es un tema con bastante perspectiva en países extranjeros, en Chile constituye una realidad desconocida y poco estudiada jurídicamente. Digamos desde ya que este tema, el de los *"datos personales o nominativos procesados computacionalmente"* va mucho más allá que el problema de los protestos, de la morosidad comercial y de los archivos históricos almacenados en bancos de datos.

En el **Capítulo II** se plantean los elementos conceptuales y doctrinarios necesarios para entender cuál es el problema de fondo que pretende solucionar el denominado *"Derecho de la Protección de Datos";*

En el **Capítulo III**, recogiéndose los elementos previamente expuestos se revisa brevemente cuál fue la tramitación parlamentaria de la ley aprobada y cuál es el contenido y los alcances de los artículos que la conforman, para cerrar los comentarios formulando algunas observaciones generales a la ley.

II. LA PROTECCION DE DATOS PERSONALES O NOMINATIVOS Y EL "HABEAS DATA". PLANTEAMIENTOS DOCTRINARIOS Y DERECHO COMPARADO.

1. Generalidades.

Suele afirmarse que el abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la intimidad, porque cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados. Esta imagen inmaterial del titular de los datos debe ser resguardada porque puede ser creada errada o dolosamente, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio.

2. El problema de fondo se origina por un conflicto entre dos intereses relevantes.

Por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc.

Por el otro, un interés –también muy legítimo- que poseen los gobiernos y los particulares para acceder a cierta información: ...los Estados para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quienes tienen SIDA al momento de fijar políticas de salud; y los particulares, generalmente constituidos en empresas de servicios o entidades gremiales, que para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial.

La respuesta doctrinaria ha sido ***la formulación de un nuevo concepto del Derecho a la Intimidad***, que surge frente a la llamada o reclamada *Libertad Informática* o de procesamiento de datos personales-nominativos; que deja

de lado el enfoque individualista o negativo con que fue concebido para plantearse desde una perspectiva socializadora y positiva (ya no es "el derecho a ser dejado a solas"); y que se concibe como *la posibilidad de que los ciudadanos titulares y propietarios de los datos que les conciernan controlen el uso y el eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente.*

3. Solución al problema de determinar qué antecedentes forman parte de la llamada "esfera privada" y cuáles de la "esfera pública" de las personas.

Los órganos estatales y las empresas comerciales que a partir de nuestro número de identificación nacional procesan información personal, se han preocupado de aclarar que ellos sólo estarían manejando o procesando ciertos "datos públicos". Esto es delicado, porque el límite entre la esfera privada y la esfera social o pública de una persona no se ha establecido legalmente con claridad, y porque el problema de los cotidianos atentados contra la vida privada, la igualdad laboral, la igualdad ante la ley y la libre iniciativa en materia económica -para nombrar algunas garantías fundamentales afectadas- surge cuando se cruzan computacionalmente y con toda facilidad antecedentes personales y se elaboran perfiles.

En la medida que un particular consienta o una norma legal establezca que ciertos datos o antecedentes personales sean susceptibles de conocerse[1]*, éstos pasarán a formar parte de una esfera social o pública porque lo vincularán con la sociedad. En el caso contrario, esto es, si cada titular de los datos que lo individualizan opta por mantenerlos reservados o no existe una ley que por razones de orden público permita expresamente conocerlos*[2]*, tales antecedentes, que les pertenecen*[3]*, serán parte de una esfera íntima o reservada que no puede ser atisbada, procesada o conocida por particulares, por empresas que quieran comercializarlos e incluso por órganos estatales. Dichos datos en Chile están protegidos por la esfera íntima que consagra la garantía del artículo 19 N°4 de la Constitución.*

4. "Derecho de Acceso o Habeas Data".

Se produce -doctrinaria y legalmente- la conciliación entre el Derecho a la Intimidad y el Derecho a la Información a través del control que para el titular de los datos posibilita el denominado ***"Derecho de Acceso"*** o ***"Habeas Data"***, una nueva garantía fundamental (o un nuevo mecanismo de resguardo y tutela) que contemplan en el Derecho Comparado tanto algunas Cartas Fundamentales como las llamadas Leyes de Protección de Datos, y una consagración del ***"Principio de la Autodeterminación Informativa".*** El *"Habeas Data"* es una acción cautelar de rango constitucional, heredera de otro recurso y tan importante como el *"Habeas Corpus"*, que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales -al decir de una sentencia histórica del Tribunal Constitucional alemán- "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente.

5. ¿Cómo logran las Leyes de Protección de Datos, vigentes desde hace 20 años en el Derecho Comparado, el equilibrio de los intereses involucrados?.

Básicamente de la siguiente forma: no niegan la posibilidad del procesamiento o tratamiento de datos, pero consagran facultades de acceder, corregir, actualizar o eliminar datos para los titulares de los mismos (enmarcadas en el denominado *"Habeas Data"*); establecen mayores limitaciones para el procesamiento cuando los datos son de especial relevancia como los llamados "sensibles" o "personalísimos" (vida sexual, salud, raza, credo religioso, filiación política, etc); regulan separadamente el procesamiento que realice un órgano público, una persona natural o una persona jurídica, estableciendo diferentes requisitos de constitución; regulan acabadamente las obliga-

---

[1] *Pensemos en los siguientes datos: número de teléfono; profesión; filiación política; origen étnico; situación laboral; cotizaciones previsionales;* monto de impuestos declarados; créditos bancarios obtenidos; viajes realizados; valores transados en la Bolsa; participaciones en sociedades; etcétera.

[2] Tal es el caso del prontuario o registro de condenas, de la base de datos del Servicio de Registro Electoral, del Boletín Comercial de la Cámara de Comercio de Santiago, etcétera.

[3] A propósito de los datos patrimoniales, desde 1929 a la fecha la Superintendencia de Bancos ha sostenido que uno de los atributos del dominio lo constituye la facultad exclusiva del dueño para permitir o impedir a terceros que se impongan o no de sus negocios.

ciones y prohibiciones del responsable de un sistema; la operatividad de todas las normas descansa en un órgano autónomo de control y fiscalización, "a priori" -autorizando a procesar y fijando los requisitos para hacerlo- y "a posteriori" -conociendo de los reclamos y sancionando-; y configuran sanciones administrativas como multas y penales -tipifican delitos- para el caso que las normas de la ley no se cumplan.

Todas las ***"Data Protection Act"*** tienen la siguiente estructura, a saber, una parte dogmática, una parte orgánica, una parte procedimental y una parte sancionatoria o represiva. Revisemos brevemente esta estructura:

Parte Dogmática: conceptos esenciales; principios inspiradores; ámbito de aplicación; especies o categorías de datos protegidos; consagración del Derecho de Acceso o *Habeas Data* y de sus garantías derivadas; derechos, obligaciones, restricciones y prohibiciones para los responsables de los sistemas de tratamiento de datos personales; etcétera.

Parte Orgánica: autoridad ad hoc independiente, técnicamente competente y con facultades normativas, de control y fiscalización a priori y a posteriori, y sancionatorias sobre los responsables de los bancos de datos personales; existencia de un registro público de los responsables y los bancos de datos; etcétera.

Aspectos Procedimentales: instancias de reclamos de trámite y fallo rápido y breve ante el órgano ad hoc (agotamiento previo de la vía administrativa); posibilidad de recursos posteriores ante los tribunales superiores de justicia; etcétera.

Parte Represiva o Sancionatoria: cancelación de la autorización de funcionamiento y eliminación del registro; multas; tipificación de delitos.

III. ANALISIS DE LA LEY APROBADA.

1. Estructura y contenido o ideas matrices de la ley.

La Ley consta de un **Título Preliminar** sobre "Disposiciones Generales" (artículos 1º, 2º y 3º); de un **Título I** sobre "la utilización de datos personales" (artículos 4º al 11º); de un **Título II** sobre "derechos de los titulares de datos" (artículos 12º a 16º); de un **Título III** acerca de "la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial" (artículos 17º a 19º); de un **Título IV** sobre "tratamiento de datos por organismos públicos" (artículos 20º, 21º y 22º); de un **Título V** acerca "de la responsabilidad por las infracciones a esta ley" (artículo 23º); de un **Título Final** que modifica el Código Sanitario (artículo 24º); y de tres **Disposiciones Transitorias**.

En esencia, existen "datos personales" o nominativos que le pertenecen a sus titulares y que son "tratados" manual o automatizadamente, tanto por órganos públicos como por empresas o personas particulares, a quienes la ley califica como "responsables del registro o banco de datos".

La regla general formalmente declarada por el texto legal es que dicho "tratamiento de datos personales" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" (por lo cual no se requiere de autorización para su tratamiento) y se consagran importantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera declaración de principios.

El mecanismo de resguardo recogido parcialmente del Derecho Comparado se denomina "Derecho de Acceso" o "Habeas Data", y éste, después de ejercerse ante quien aparezca como responsable sólo puede reclamarse ante los tribunales ordinarios de justicia.

2. Ámbito de aplicación.

A este respecto, el *artículo 1º* establece que se sujetará a las disposiciones de esta ley ***el tratamiento de los datos de carácter personal***, definidos por el *artículo 2ª* como los relativos a cualquier información concerniente a

personas naturales identificadas o identificables, contenidos en registros o bancos de datos y procesados tanto por organismos públicos como por entidades particulares.

2.1 Situación de las personas jurídicas como titulares de datos o sujetos de tratamiento automatizado.

Nada dice la ley respecto a los datos "personales" de las personas jurídicas, las que también poseen atributos de su personalidad, aunque su naturaleza jurídica emane de una ficción legal. Ellas son sujetos de información cuyos antecedentes también son "tratados" computacionalmente, y por definición quedan al margen de la ley que sólo rige en relación a "titulares" personas naturales. Estimamos que si bien en menor amplitud que las personas naturales, las personas jurídicas también gozan de un necesario derecho a la confidencialidad o reserva de los antecedentes que a ellas se refieren, por cuanto éstos las convierten en sujetos de derechos y en personas identificadas e identificables. En la realidad actual del procesamiento de datos, no se explica como el legislador no consideró de manera alguna esta situación.

2.2 Ámbito de aplicación de la ley desde la perspectiva de los "Responsables de las Bases de Datos".

La Ley distingue lo que es el procesamiento de datos personales al interior de la Administración Estatal o en el Sector Público y lo que ocurre en el sector privado o respecto al tratamiento por particulares, sean éstos personas naturales o jurídicas.

Respecto a **las bases de datos públicas o administradas por organismos públicos**, la ley contempla un Título específico -el IV-, compuesto por los artículos Nº20, 21 y 22. Para efectos de este informe cabe indicar que el artículo 22 contempla la obligación de que sea el Servicio de Registro Civil el ente que llevará un Registro Público de Bancos de Datos, pero sólo en relación a entes estatales y excluyendo de la obligación de registro a las empresas particulares. Esta disposición, fruto de una indicación presentada por el Ejecutivo durante el debate en Comisión Mixta ya que se trata de una materia de iniciativa exclusiva del Presidente, es de difícil comprensión, porque en sí no lleva envuelta el establecer una instancia o grado de fiscalización alguno, que es la razón de ser en las leyes de protección de datos de la existencia de órganos ad hoc[4]. ¿Cuáles son las sanciones a aplicar al órgano público que no se registre?; ¿puede el Servicio de Registro Civil realizar algún control al efecto y con qué facultades, si en Derecho Público sólo puede hacerse aquello que esté expresamente permitido?.

Nunca se entendió la importancia de que la ley contemplara un órgano de fiscalización y la existencia de un registro ad hoc. Inicialmente no se abordó el tema bajo el débil argumento de "no querer ser burocráticos"; posteriormente se propuso que fuera la Contraloría General de la República[5]; luego se estableció (en el proyecto aprobado en el Senado) que sería un órganismo público el encagado de llevar un registro de los bancos de datos tanto públicos como privados; la solución final elaborada en la Comisión Mixta para hacer el sistema aún menos restrictivo para las empresas dedicadas al procesamiento de información, es insuficiente, porque ni siquiera incluye la obligación de registro para empresas o personas privadas.

3. Breves comentarios a las definiciones.

El *artículo 2º* define 16 conceptos, no siendo las definiciones lo suficientemente claras.

---

[4] Para entender la importancia y la operatividad práctica del tema, véase en Internet la dirección www.ag-protecciondatos.es/regis.html, que *conecta con el Registro General de Protección de Datos existente desde 1992 en España.*

[5] En un informe presentado al Senado en Mayo de 1998 reparamos esta iniciativa por inconstitucional. lo que fue acogido, según consta en las páginas 36 y 37 del informe final de la Comisión de Constitución, Legislación y Justicia del Senado.

Respecto de los datos se define cuando son "caducos"[6], "estadísticos"[7], "de carácter personal"[8] o personal "sensible"[9].

Respecto de las actividades de que pueden ser objeto los datos personales, el término más amplio que se define es "tratamiento de datos"[10], y derivados de este, los conceptos de "almacenamiento"[11], "bloqueo"[12], "comunicación o transmisión"[13], "eliminación o cancelación"[14], "modificación"[15] y "procedimiento de disociación"[16].

En relación a lo que podemos denominar la infraestructura del procesamiento de datos personales, el artículo define, como veremos, lo que es un "registro o banco de datos", el "responsable del registro o banco de datos", el "titular de los datos" y los "organismos públicos".

4. "Fuentes accesibles al público".

Una novedad de la ley chilena es la incorporación en términos amplísimos, a diferencia de la Ley Española[17], *del concepto de "fuentes accesibles al público" en la letra i) del artículo 2°, las que legalmente han sido transformadas en la regla general. Se definen amplia y ambiguamente como "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado (es decir permitido) ...a los solicitantes".*

La consecuencia práctica de esta norma es que al ser los datos legalmente públicos, cualquiera puede procesarlos y comercializarlos, validándose definitivamente el lucrativo negocio de la venta de datos personales.

La primera cuestión a dilucidar es determinar cuáles son los registros *"de datos personales públicos o privados de acceso no restringido o reservado a los solicitantes"*, porque los que no detenten esta calidad, aquellos cuyo acceso sea permitido, constituirán fuentes accesibles al público. La Ley no hace una categorización. No creemos que se trate de una cuestión meramente de hecho, sino que dicha determinación sólo podrá hacerse por los órganos jurisdiccionales pero para casos concretos. No obstante, ya en Chile existen algunas fuentes de información que son de acceso restringido ya que existen leyes que previamente así lo han establecido al darle a los datos el carácter de reservados o confidenciales. Nos referimos a lo menos al secreto estadístico (IN), al secreto tributario, al secreto bancario o al secreto de la filiación política. Al existir tales normas, son de acceso restringido; si no existieran (que es la regla general) serían de acceso permitido o fuentes públicas.

---

6 Conforme lo establece la letra d) del artículo 2º, "dato caduco" es el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

7 Letra e): ...dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

8 Letra f): ...datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

9 Son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

10 Es cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

11 Se entiende por tal a conservación o custodia de datos en un registro o banco de datos.

12 Consiste en la suspensión temporal de cualquier operación de tratamiento de los datos almacenados

13 La Comunicación o transmisión de datos es dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

14 Es la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

15 Consiste en todo cambio en el contenido de los datos almacenados en registros o bancos de datos

16 Se entiende por tal a todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

17 El artículo 28 de la Ley Española ya anotada, regula las fuentes accesibles al público solamente con el objeto de establecer que de esta clase de registros o bancos de datos pueden obtenerse datos patrimoniales positivos, dejando fuera de su alcance a los demas datos, especialmente a los sensibles. En tal Ley y las normas complementarias dictadas por la Agencia de protección de Datos se entiende por "datos accesibles al público" aquellos que se encuentran a su disposición en forma general y no impedidos por cuelquier norma limitativa (por ejemplo, datos de censos, anuarios, repertorios de jurisprudencia, archivos de prensa, guías telefónicas, etc.).

Cabe sentar la siguiente conclusión: en Chile todas las fuentes de datos personales serán de acceso público, no restringido o reservado a los solicitantes, salvo que una ley establezca expresamente lo contrario.

5. Análisis del artículo 4º[18].

Ubicada en el Título I sobre la utilización de datos personales, se trata de la norma más conflictiva y confusa, misma que, en nuestra opinión, es clave para entender que estamos frente a una normativa que apuntó a proteger y legalizar el negocio del procesamiento de datos personales desde la perspectiva de las empresas del ramo, más que a resguardar los derechos de los titulares a quienes aluden o a quienes se refieren los datos personales o nominativos.

5.1 Regla general.

El artículo sienta un principio general en materia de procesamiento de datos personales, el que, atendidas las excepciones que luego consagra, no es sino una mera "declaración de principios". Señala que ***el tratamiento de los datos personales sólo podrá efectuarse cuando esta ley u otras disposiciones legales lo autoricen, o cuando el titular consienta expresamente en ello.***

5.2 Excepciones.

La norma consagra diversas excepciones en los incisos quinto y sexto, en relación a la autorización del titular requerida para el tratamiento de los datos. Establece que en determinados casos ***no requiere autorización el tratamiento de datos personales que provengan o que se recolecten de "fuentes accesibles al público" (que ya sabemos son, por definición, la regla general).***

a) Cuando sean de carácter económico, financiero, bancario o comercial.

b) Cuando se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento.

c) Cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Si bien es cierto que desde un punto de vista comercial aparece conveniente la relación directa entre una empresa y sus clientes, la posibilidad de decidir que dicha relación exista o no, le compete a los consumidores, los que pueden desear mantenerse al margen y resguardar la privacidad de sus datos personales para no ser invadidos con agresivas campañas comerciales o promocionales y recibir *e-mails*, cartas, folletos o llamados telefónicos, y así debiera garantizarse jurídicamente.

---

18 Artículo 4°. El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito.

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

La ley aprobada legaliza con mínimas limitaciones el marketing directo. El artículo 4º en comento establece como amplia excepción y perentoriamente, que no se requiere autorización para el procesamiento de datos personales que provengan de fuentes públicas cuando sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, lo que, sumado a las dos excepciones anteriores o perfilados con los datos a que ellas aluden, declara exento de autorización o control para el titular a un cúmulo demasiado grande de datos nominativos o personales[19].

d) Cuando el tratamiento de datos personales lo realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

6. La relevante figura del "responsable del registro o banco de datos personales".

La letra n) del *artículo 2°* señala que reviste tal calidad *"la persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal".*

El mismo artículo define lo que debe entenderse por "registro o banco de datos", a saber, *"el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos".*

El *artículo 5°* faculta al responsable para establecer un procedimiento automatizado de datos personales.

El *artículo 6°* señala que el responsable tiene la obligación de eliminar, modificar o bloquear datos personales sin necesidad de requerimiento del titular (léase "de oficio").

El *artículo 11°* establece que el responsable de los registros o bases de datos personales deberá cuidar de ellos con la debida diligencia. Obviamente agrega que lo hará "con posterioridad a su recolección" y que se hará responsable de los daños producidos. Entendemos, en consecuencia, que responde de la culpa leve.

El *artículo 12°* lo indica como la persona ante quien se ejerce el denominado *"Habeas Data"* o *"Derecho de Acceso".*

El *artículo 16°* señala que su domicilio determina la competencia de los tribunales.

El artículo 17° faculta al responsable, en las condiciones que más adelante se verá, para comunicar a terceros los datos patrimoniales negativos.

Un comentario final respecto del responsable: atendido que la ley eliminó la obligación que los responsables queden anotados en un registro público, es factible que los titulares de los datos personales nunca sepan de la existencia del banco de datos o el origen de los datos y que los responsables actúen en total anonimato y carentes de toda fiscalización por la autoridad.

7. El "Habeas Data" o "Derecho de Acceso".

Esta garantía esencial de toda ley de protección de datos y las facultades que de ella derivan, mismas que por su importancia en varios países tienen rango constitucional, están reguladas en los *artículos 12º, 13º, 14º* y *15º* de la ley, que son los primeros del Título II sobre "Derechos de los titulares de datos", y se ejercen precisamente ante quien aparezca como responsable del registro.

En síntesis, la ley establece inicialmente que ***toda persona tiene derecho a exigir -a quien sea responsable de un registro banco de datos que se dedique en forma pública o privada al tratamiento de datos personales-, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.***

De esta declaración inicial del derecho de ***"acceder a la información"***, se derivan una serie de garantías o de facultades correlativas.

La ***"modificación"*** de los datos personales procede cuando sean erróneos, inexactos, equívocos o incompletos, y así se acredite.

La ***"eliminación"***, salvo las excepciones legales, puede exigirse, en caso que el almacenamiento de datos personales carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de ***"bloqueo de los datos"***, puede hacerse cuando se hayan proporcionado voluntariamente los datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

Aproximaciones para una Propuesta Legal en Materia de Medidas Seguridad Aplicable a la Contratación Electrónica en el Perú

Autor: **José Francisco Espinoza Céspedes (Perú)**

CURRICULUM:

- Abogado egresado de la Facultad de Derecho y Ciencias Políticas de la Universidad de Lima. Con estudios de Post Grado en "Comercio Electrónico en la Gestión de los Negocios Internacionales". Universidad Nacional Mayor de San Marcos. Jefe de Práctica del curso de Legislación en la Facultad de Ingeniería de Sistemas de la Universidad de Lima (1998-1999).

SUMILLA:

"El uso de medidas de seguridad en la contratación electrónica se presenta como una de las necesidades básicas para el desarrollo de las operaciones en el Ciberespacio en tal sentido, mediante el uso de las herramientas que nos permite el Derecho Informático y el Análisis Económico del Derecho, se plantea la necesidad de legislar el tema en el Perú.

Seguidamente se exponen los lineamientos básicos que puedan servir de base al legislador para implementar una norma que permita que las operaciones se efectúen en un medio seguro, de tal forma que se eviten perjuicios a quienes manifiesten su voluntad por medios electrónicos.

Finalmente se concluye, entre otras, que el sistema legal que se adopte en un entorno de contratación electrónica, deberá considerar tecnologías abiertas o neutrales que no generen trabas legales para su desarrollo en el país."

1. INTRODUCCION.

Los elementos tecnológicos están en constante desarrollo y expansión, estas circunstancias unidas al rápido crecimiento de las telecomunicaciones, permiten que el ser humano tenga mayores posibilidades de interactuar con sus semejantes, desde los lugares más distantes del planeta. Esta realidad que por su naturaleza es compleja, se presenta como un medio con gran capacidad para dañar, perjudicar o simplemente incomodar al usuario de éstas tecnologías, que se encuentre desprevenido o desinformado sobre los peligros de usar sistemas tecnológicos sin las respectivas medidas de seguridad; en este sentido surge la imperiosa necesidad para la intervención del Derecho como regulador de las conductas de los individuos en la sociedad, a fin de plantear las normas mínimas de seguridad que hagan viable la convivencia social.

Ante a esta situación que debemos enfrentar, surge el Derecho Informático[1], como rama autónoma del Derecho, para plantear instituciones y desarrollos doctrinarios que otorguen al operador legislativo las herramientas legales que le permitan tomar decisiones adecuadas para prever y plantear soluciones a los grandes problemas de inseguridad que se vienen presentando en el Ciberespacio. En este orden de ideas, en el Perú se viene trabajando para dotar al país de una legislación jurídico informática que apoye el desarrollo de operaciones seguras en un entorno electrónico o digital.

[1] "El derecho informático es la aplicación de las instituciones jurídicas para resolver los problemas que plantea la informática. El Derecho informático es una disciplina inequívocamente jurídica que comprende un conjunto amplio de soluciones jurídicas en forma coherente y sistemática." Nuñez Ponce Julio. Software: licencia de uso, derecho y empresa. Fondo Editorial de la Universidad de Lima. Lima,. 1998, p.63. así mismo se dice que "el Derecho Informático o Derecho de la Informática se refiere a los problemas jurídicos que se originan en la sociedad por el uso de la computadoras" Nuñez Ponce Julio. Derecho informático. Nueva Disciplina para una sociedad moderna. Marsol Perú Editores S.A. Trujillo. 1ra. Edición, p.21.

2.- ASPECTOS GENERALES ENTORNO A LA CONTRATACION ELECTRONICA.

La contratación electrónica se presenta al mundo como una nueva forma de intercambiar bienes y servicios. Por el constante avance tecnológico, la confianza que le brindan los agentes económicos, la importancia y trascendencia que va alcanzando para el desarrollo de la sociedad, etc., la convierten en materia de interés jurídico, en vista que es llamada a ser uno de los aspectos fundamentales para la creación de riqueza en la sociedad.

La Contratación electrónica, es la que se efectúa a través de cualquier medio electrónico que "tiene, o puede tener,[...] incidencia real y directa sobre la formación de la voluntad [...], el desarrollo o [la] interpretación futura del acuerdo."[2]. En esta forma de interactuar, el contacto presencial entre las partes desaparece, surgiendo una interacción electrónica.

Este nuevo medio permite que desde cualquier parte del mundo se pueda contratar en segundos; en tal sentido la manifestación de voluntad de los interesados trasciende sus fronteras de origen para dar vida y crecimiento al mercado más competitivo y eficiente de todos los tiempos, por lo que surge como una realidad innegable, el concepto de Aldea Global.

Es fundamental que las operaciones efectuadas por medios electrónicos cuenten con las debidas medidas de seguridad tanto desde el punto de vista técnico como legal, para evitar que personas ajenas a la relación electrónica entre las partes, se vean tentadas a interceptar las transacciones por medios electrónicos, u análogos.

La importancia de la contratación electrónica radica en que ésta permite un ahorro de tiempo y dinero, haciendo que las operaciones entre los interesados sean más dinámicas, eficientes y libres de intermediarios, circunstancias que permitirán la creación del mercado electrónico.

Frente a los hechos que estamos atravesando es de vital importancia dedicar tiempo y esfuerzo a encontrar los mecanismos legales que brinden la seguridad a los interesados en manifestar su voluntad por medios electrónicos.

3.- NECESIDAD DE SEGURIDAD EN LA CONTRATACION ELECTRONICA.

Por el desarrollo tecnológico alcanzado, se ha logrado la interacción entre computadoras, situación que nos permite estar en condiciones de transmitir a distancia millones de datos, información, bienes y servicios, etc., resultando de ello la contratación electrónica y sus diversas aplicaciones, por ejemplo en el transporte de mercancías e *información; en el comercio en general; en el ámbito financiero y en casi todas las actividades del ser humano debi*do a las facilidades para la transmisión, emisión y recepción de señales, imágenes, sonidos de todo tipo, por medio de diferentes elementos como los cables de cobre, cables coaxiales, y fibra óptica[3]; por esta diversidad de medios de transporte se logra el complemento ideal entre la contratación electrónica y los servicios de telecomunicaciones[4], acelerándose el proceso de expansión de la contratación electrónica, a todas las áreas del quehacer humano.

---

[2] Dávara Rodríguez. M. A. Manual de Derecho Informático. Editorial Aranzadi Pamplona, 1997, p. 165.

[3] "Las fibras ópticas con la gran capacidad de ancho de banda que proporcionan y su bajo coste de mantenimiento, han permitido bajar hasta límites insospechados el [precio] de la transmisión de señales (en ocasiones incluso resulta menos costoso levantar la planta de cobre de una ciudad entera y sustituirla por fibra óptica que mantener esta durante algunos años) [...] al llegar la fibra óptica cada vez más cerca del usuario, acerca a éste a una red con un enorme potencial de ancho de banda, abriendo paso a nuevos servicios, superando las restricciones tradicionales del par de cobre." CANALEJO, Miguel Ángel. Evolución de Infraestructuras. En: Telecomunicaciones 1996. Informes anuales de Fundesco. Fundesco. Madrid, 1996, p. 173.

[4] " Hasta hace poco, la tecnología de las telecomunicaciones obligaba a construir redes independientes para atender a las diferentes necesidades de los servicios de telecomunicación. En la actualidad no pasa un solo día que aparezca un nuevo teleservicio [...] o una nueva alianza que busca obtener una ventaja de la tan repetida sinergía entre el ordenador y las telecomunicaciones." GODEROS, Antonio. Los Retos de la Sociedad de la Información: impacto de la nueva infoestructura. En: Telecomunicaciones 1996. Informes anuales de Fundesco. Fundesco. Madrid, 1996, p. 213.

Los elementos electrónicos, en unión con las redes de telecomunicaciones, han permitido la creación de una zona donde las personas pueden relacionarse sin estar físicamente presentes creándose un nuevo espacio para la contratación electrónica, denominado Ciberespacio, que para Klaus Bartels es el "Espacio en el que no hay ya "derecha" ni "izquierda", "arriba" y "abajo" [...], sobre todo no, existe más "cerca" ni "lejos". [...]. Sólo que los trotamundos del CiberEspacio [...] ya no son caminantes que pasean [...] sino "surferos" que espacian [...] en el octavo mar, el de las olas de la información"[5], y para Nora Dominique, es " [...] un nuevo espacio relacional donde los individuos, [...], conversan e intercambian datos por medio de terminales y redes entrelazadas. Este espacio de comunicación virtual, que se encuentra más allá de nuestras pantallas y nuestras tomas telefónicas, constituye aquello que [...] William Gibson llamaba *cyberspace* en su novela newromancer "[6]

La contratación electrónica permite la apertura de las redes a infinidad de personas, en los diversos puntos del planeta para el intercambio de bienes y servicios formándose en la mayoría de los casos, las sociedades electrónicas al servicio de la ciencia, la cultura, la economía y la sociedad en general. Este mismo entorno que presenta muchas oportunidades para la humanidad es frecuentado por sujetos capaces de ingresar violentamente a los Centros de Cómputo, rompiendo o alterando los sistemas de seguridad para navegar, copiar, alterar o robar información confidencial de bases de datos y las redes en general; son los llamados Hacker, Crakers, Phreakers,etc.; por eso se dice que "[...] el ciberespacio, lejos de ser un campo de juego para marginados y tecnoperversos, constituye un entorno que tiene el potencial para transformar nuestra vida futura. Las condiciones en que los ciudadanos tendrán acceso a él y los servicios públicos y privados que ofrecerá, los modos en que se administrarán las redes y se organizará el comercio y la libertad de expresión, en que se protegerá o no la vida privada y la propiedad intelectual, ejercerán una influencia decisiva en nuestra civilización"[7]

Dentro de esta perspectiva es importante recalcar que el comercio electrónico[8] y la contratación electrónica en general, vienen cambiando muchas de nuestras costumbres en el ámbito de la transferencia de bienes y servicios, los sistemas de pago, las transacciones en línea, etc.; que hacen indispensable la adopción de medidas de seguridad, tanto técnicas como legales.

La seguridad es uno de los problemas fundamentales que interfieren con el desarrollo de la contratación electrónica, por esta razón todos los países deben tomar las medidas correctivas a fin de evitar que desconocidos alteren los contenidos, las manifestaciones de voluntad y el orden de las redes en general. Frente a tales circunstancias es necesario contar con legislación que regule en forma armónica y uniforme las medidas de seguridad que se deben adoptar para enfrentar las tales hechos.

4.- EL ANALISIS ECONOMICO DEL DERECHO FRENTE A LAS MEDIDAS DE SEGURIDAD APLICABLES A LA CONTRATACION ELECTRONICA.

Las medidas de seguridad aplicables a la contratación electrónica como base para la creación de un nuevo mercado, pueden ser estudiadas por el Análisis Económico del Derecho, para comprender la importancia de la contratación segura, como un sistema eficiente para la asignación de recursos a nivel global. Este método económico, con su especial forma de enfocar los problemas sociales y jurídicos tiene sus antecedentes en la idea de maximizar beneficios al menor costo; sin embargo sobre la base de los trabajos de Ronald Coase se logra sistematizar con rigor académico, el Análisis Económico del Derecho. Como fruto de estas investigaciones Coase logró desarrollar un conjunto de elementos teóricos conocidos como el teorema de Coase, que le permitieron ganar el premio novel de economía en el año 1991.

---

[5] Texto traducido del Alemán por Aurelio Mini. Mini Aurelio. ¿Por qué Internet ... y no más bien nada? Artículo integrante de la obra de: Maúrtua J. y otros. Proyecto de Filosofía Aplicada. Asociación Cultural y Educativa Búho Rojo. Ediciones Espigón. Lima. 1998, p. 139.

[6] Dominique, Nora. La Conquista del Ciberespacio. Editorial Andrés Bello. Santiago de Chile, 1997, p.20.

[7] Ibidem, p. 20.

[8] Creemos necesario indicar que el comercio electrónico por estar destinado única y exclusivamente a operaciones comerciales, representa un elemento incluido dentro del concepto de contratación electrónica que engloba cualquier manifestación de voluntad, sean estas de carácter contractual o no.

Una de las necesidades sociales que pone en aprietos a los investigadores son las medidas de seguridad, que aplicadas a la contratación electrónica permitan el desarrollo de un mercado electrónico que no sea vulnerable al ataque de terceros ajenos a las partes, por lo que es necesario establecer medidas de seguridad informáticas que sean aplicables a las relaciones entre las partes que intervienen en este mercado, siempre dentro de un marco de legalidad, en vista que las leyes representan los ideales de justicia de la sociedad.

Como el mercado electrónico no se encuentra en equilibrio perfecto, el Derecho cumple un rol importante, en la corrección de los problemas de costo y beneficio, en defensa del entorno social al dar el equilibrio necesario a través de la corrección de las externalidades inherentes a todo mercado, de las cuales no se puede librar el mercado electrónico. El Derecho a través de la norma, debe intervenir distribuyendo los costos y beneficios, en busca de la solución eficiente.

Dentro de esta perspectiva de análisis, debemos concentrar nuestra atención en el teorema de Coase, que en su primera versión plantea que "si hubiera unos costes de transacción cero, se produciría el resultado eficiente con independencia de la norma atributiva de derechos elegida"[9] Esta primera parte del teorema se aplicaría para un mercado perfecto en donde los costos de transacción, incluyendo las medidas de seguridad aplicables a la contratación electrónica fueran cero, en este supuesto el mercado a través de sus mecanismos lograría obtener la solución más eficiente; sin importar cual de las partes interesadas tome la iniciativa en la aplicación de las medidas de seguridad, creando un mercado donde la seguridad sea la constante común por ser una acción eficiente.

De acuerdo a la primera parte del parte del teorema de Coase, cuando los costos de transacción son iguales a cero, es irrelevante que se usen o no medidas de seguridad en la contratación electrónica, por que el mercado dará la solución eficiente.

El teorema de Coase, presenta una segunda parte que plantea que "si hubiese costes de transacción positivos, la solución eficiente no podrá producirse con independencia de la norma jurídica elegida"[10], esta es la manera como se desarrollan las actividades diarias en la sociedad, debido a que aún no existen transacciones donde los costos sean iguales a cero.

El uso de medidas de seguridad en la contratación electrónica es una solución eficiente, permitiendo que el mercado electrónico adquiera su real importancia y cumpla con el rol al servicio a la sociedad que le ha tocado prestar. Corresponde a la ley hacer obligatorio el uso de medidas de seguridad adecuadas a la contratación electrónica, en vista de la incapacidad del mercado para dar una solución al respecto, por los altos costos en que deberían incurrirse, para dar una solución eficiente por este medio. Es por eso que "El teorema de Coase [...], es la base para analizar, con apoyo económico, las consecuencias de disposiciones jurídicas alternativas y para justificar las propuestas de modificación de normas jurídicas"[11]

En tal sentido, el teorema de Coase sirve de base para el análisis de las medidas de seguridad aplicables a la contratación electrónica, es por eso que investigadores como Roemer[12] señalan que Coase demostró el efecto de los costos de transacción sobre las normas, facilitando un elemento indispensable para el análisis económico de los derechos. De otro lado Polinsky[13] plantea que con hipótesis realistas (en directa alusión a la segunda parte del teorema) sobre los costos de transacción, una norma sería preferible a otra por motivos de eficiencia, al proporcionar criterios para la elección de las normas jurídicas que sean adecuadas al tema en estudio.

5.- APROXIMACIONES A UNA PROPUESTA LEGAL EN MATERIA DE MEDIDAS DE SEGURIDAD APLICABLES A CONTRATACION ELECTRONICA EN EL PERU.

Para una propuesta legal que regule las medidas de seguridad aplicables a la contratación electrónica en el Perú, creemos conveniente que se deben tener en cuenta los siguientes criterios:

---

9 Polinsky Mitchell. Introducción al análisis económico del Derecho. Editorial Ariel S.A. Barcelona. 1ra. Edición, 1985, p. 24.
10 Polinsky Mitchell. Introducción al análisis económico del Derecho. Editorial Ariel S.A. Barcelona. 1ra. Edición, 1985, p. 25.
11 Schafer, Hans-Bernar. Manual de Análisis Económico del Derecho Civil. Editorial Tecnos. S.A. Madrid, 1991, p. 85.
12 Roemer, Andrés. Introducción al Análisis Económico del Derecho. Fondo de Cultura económica. México, 1994, p. 09.
13 Polinsky Mitchell. Introducción al análisis económico del Derecho. Editorial Ariel S.A. Barcelona. 1ra. Edición, 1985, p. 26.

a) Delimitar claramente el ámbito de aplicación de la norma, donde se deberá establecer que las medidas de seguridad se aplicarán a todo tipo de transacción, sean éstas públicas o privadas, independientemente de su naturaleza. Debiendo dejarse expresamente establecido que esta ley complementará a otras leyes relacionadas con el tema, salvo que se mencione lo contrario.

b) Presentar definición de términos en la que conste claramente lo que se entiende por medida de seguridad, contratación electrónica, firma electrónica, firma digital, firma biométrica, técnicas de cifrado, clave pública y privada, documento electrónico, certificado, suspensión, revocación, entidad de certificación, etc., en vista que se trata de regular una materia donde los términos técnicos son una constante.

c) Plantear que los resultados de actividades electrónicas, similares u análogas tienen pleno valor y efecto legal si se cumple con todos los requisitos técnicos y jurídicos que permitan su integridad, autenticidad, confidencialidad, no rechazo y disponibilidad; prohibiéndose toda exclusión procesal por el hecho de su formación o presentación electrónica. Para efectos del pleno valor probatorio, se deberán cumplir con las exigencias mínimas que exige la ley.

d) Crear una Superintendencia para la Contratación Electrónica, que se encargue en forma autónoma por el cumplimiento de la ley de la materia. Esta institución deberá contar entre otras, con las siguientes funciones: emitir, suspender y revocar certificados; regular el establecimiento de entidades de certificación, supervisar y autorizar el uso de sistemas de seguridad, elaborar manuales para los procedimientos de certificación, fiscalización, etc., y todas aquellas que le sean necesarias para el cumplimiento de sus fines.

e) Autorizar el uso de firmas electrónicas, digitales, biométricas; entidades de certificación: obligaciones, prohibiciones, formas de fiscalización, etc.

f) Diseñar un régimen específico aplicable a los certificados: emisión, revocación, suspensión, vigencia, límites de responsabilidad, garantías; evaluación de solicitudes y otorgamiento de licencias para el funcionamiento de bases de datos, etc.

g) Delimitar lo relacionado con el deber de secreto que deben cumplir las entidades de certificación, en el ejercicio de sus funciones.

6.- CONCLUSIONES.

La contratación electrónica se va difundiendo en todo el mundo; esta forma de transar con adecuadas medidas de seguridad se perfila como uno de los medios más importantes para el desarrollo de actividades generadoras de bienes y servicios. Por este sistema se moverá la mayor parte de la riqueza en la sociedad, hecho ante el cual no debemos mostrar indiferencia.

Por los grandes beneficios que trae consigo la contratación electrónica segura, es de vital importancia que en el Perú se legisle de manera sistemática y armónica, todo lo relativo a la inserción de normas mínimas de seguridad aplicables a las actividades en el Ciberespacio, como medio de fomentar la inversión y el uso de éstas tecnologías en beneficio de nuestro país y de la sociedad en su conjunto.

El uso de medidas de seguridad en la contratación electrónica se ha convertido en necesidad y a la vez en una solución eficiente, que permite hacer frente al problema de las intrusiones, estas medidas deberán reforzarse con la adecuada regulación Penal, de tal forma que quienes alteren el orden en el Ciberespacio, sean sancionados drásticamente; de tal forma que la contratación electrónica segura genere confianza entre los usuarios.

En el Perú, es necesaria la creación de una Superintendencia para la Contratación Electrónica que se sirva de nexo y garantía para el desarrollo de políticas que faciliten las operaciones seguras en el Ciberespacio. Esta institución

deberá crear las condiciones necesarias para que las empresas prestadoras de servicios operen con los requisitos mínimos de seguridad que imponga la ley respectiva, además de servir de contacto con sus similares en el mundo.

El sistema legal que se adopte para el uso de medidas de seguridad aplicables a la contratación electrónica, deberá considerar tecnologías abiertas o neutrales que permitan el avance del estado de la ciencia y de la técnica, previéndose que no se generen trabas legales para su desarrollo en el país.

Es fundamental la armonización de las leyes sobre medidas de seguridad aplicables a la contratación electrónica que se encuentran dispersas en el ordenamiento jurídico peruano, para uniformizar las normas que permitan otorgar plena validez y efectos jurídicos a las transacciones electrónicas seguras.

La Libertad Informática: Derecho Fundamental en la Constitución Venezolana

Miriam Álvarez B. de Bozo (*) / Flor María Ávila Hernández (*) / Héctor Ramón Peñaranda Quintero (*)
(Venezuela)

Universidad del Zulia (LUZ). Maracaibo. Venezuela.
Organización Mundial de Derecho e Informática (OMDI). Maracaibo. Venezuela.

RESUMEN

Esta investigación tiene como propósito analizar las amenazas y los riesgos a las cuales está expuesta la vida privada de las personas en la sociedad de la información, en particular, aquellas derivadas del tratamiento de los datos personales a consecuencia de la utilización de las nuevas tecnologías de la información, así como determinar cuál debe ser el rol del ordenamiento jurídico constitucional ante el referido problema. Para tal fin, se analizó el estado actual de la tecnología y se realizó un estudio de la legislación, doctrina y jurisprudencia nacional y comparada que permitió desarrollar el nuevo contenido del derecho a la privacidad con relación al derecho a la libertad informática así como la justificación de éste último como nuevo derecho fundamental de tercera generación. Se concluye que la incorporación del derecho a la libertad informática en la novísima Constitución Nacional de la República Bolivariana de Venezuela de 1.999 representa un considerable avance en la protección de la intimidad y vida privada de los individuos, con lo cual nuestro Constituyente se articula con la tendencia y recientes criterios sobre la materia de las Constituciones Latinoamericanas de las últimas décadas y de la Legislación Comunitaria Europea.

Palabras claves: *datos personales, libertad informática, regulación constitucional.*

(*) Este trabajo ha sido elaborado con los aportes de los investigadores Miriam Álvarez B. de Bozo, miembro de la Sección de Derecho Público y Directora del Instituto de Estudios Políticos y Derecho Público de la FC.JP de LUZ; Flor Ávila Hernández, miembro de la Sección de Informática Jurídica del Instituto de Filosofía del Derecho Dr. J.M. Delgado Ocando de FC.JP de LUZ, coinvestigadora del Programa de Investigación "Bases Teórico Metodológicas de la Contratación en el marco de las Nuevas Tecnologías ", (auspiciado por el CONDES) y Héctor Ramón Peñaranda Quintero, Presidente de la Organización Mundial de Derecho e Informática (OMDI)-.

Informatic Freedom: Fundamental Right in the Venezuelan Constitution

Miriam Álvarez B. de Bozo (.)
Flor María Ávila Hernández (.)
Héctor Ramón Peñaranda Quintero (*)

(.) Universidad del Zulia (LUZ). Maracaibo. Venezuela.
(*) World Organization of Law and Computer Science (OMDI). Maracaibo. Venezuela.

ABSTRACT

This investigation has the intention of analyzing the threats and risks to which the privacy life is exposed in the society of information, particularly, those derived from the treatment of the personal data as a result of the use of new technologies of information, as well as to determine which must be the roll of the constitutional legal regula-

tion against the referred problematic. For such aim, the present state of technology was analyzed and a study of the legislation, doctrines and national and compared jurisprudence was made, that allowed to develop a new content of privacy right in relation to the right of informatic freedom as well as the new justification of this one as a new fundamental right of third generation. It is concluded that the incorporation of the right of informatic freedom in the new National Constitution of the Bolivarian Republic of Venezuela represents an advancement in the protection of the intimacy and privacy of the individuals and with this fact our Constituent inserts the recent criteria related to this matter of the Latin American Constitutions of the last decades and the European Communitarian Legislation.

KEY WORDS: *PERSONAL DATA, INFORMATIC FREEDOM , CONSTITUTIONAL REGULATION.*

INTRODUCCION

La presente investigación tiene por objeto analizar las amenazas y los riesgos a las cuales está expuesta la vida privada de las personas en la sociedad de la información, en particular, aquellas derivadas del tratamiento de los datos personales a consecuencia de la utilización de las nuevas tecnologías de la información y de la comunicación, así como determinar cuál debe ser el rol del derecho ante la referida problemática.

Para tales efectos, se analiza cuál es el estado actual de la tecnología que permite el tratamiento de los datos personales y con ello, la aparición de riesgos asociados a dicho tratamiento así como se estudia la protección a la vida privada que para tales situaciones otorga nuestro ordenamiento jurídico vigente, especialmente la prevista por la normativa constitucional elaborado por la Asamblea Nacional Constituyente y recientemente aprobada por el pueblo venezolano mediante referéndum efectuado el 15-12-99, con vigencia a partir del 30-12-1999. Se identifican asimismo las soluciones aportadas por el derecho comparado.

En primer lugar, se debe señalar que la protección jurídica del tratamiento de los datos personales puede ser analizado desde varias perspectivas, la primera, la tutela que ofrece el ordenamiento jurídico interno de un Estado particular a sus habitantes y la segunda, la protección que ofrece el derecho comunitario y los organismos supranacionales a los individuos de los Estados miembros, incluyendo dentro de ésta, entre otros aspectos, la transmisión transfronteriza de los datos personales.

Ahora bien, el presente estudio se ubica dentro de la primera perspectiva, es decir, analiza cuál es la protección que nuestro actual ordenamiento jurídico otorga al tratamiento de los datos personales, entendiendo por éstos aquellos que permitan identificar a un individuo y que involucran aspectos de su vida privada. De igual forma, en este trabajo se desarrolla el ámbito global que implican las más recientes concepciones de la privacidad, incluyendo dentro de ésta, el derecho a la libertad informática, entendido como la facultad que tiene el individuo de acceder, conocer y controlar su información de carácter personal. Si bien este derecho protege un ámbito particular de la vida privada de los individuos, en este caso, sus datos personales, los grandes riesgos a la privacidad que hoy por hoy produce el tratamiento de éstos a través del uso de las nuevas tecnologías, han originado que los más modernos ordenamientos jurídicos, entre ellos, el comunitario europeo, hayan dotado de independencia y autonomía al referido derecho inclusive a sus garantías formales, en los cuales se establecen para su tutela organismos judiciales y administrativos así como la consagración de figuras garantes ad-hoc.

CIRCUNSTANCIAS QUE PROMUEVEN Y JUSTIFICAN EL DERECHO FUNDAMENTAL A LA LIBERTAD INFORMATICA.

1.- La aparición de la telemática, producto de la concurrencia de las telecomunicaciones y la informática, a finales de la década de los 70. Esta nueva tecnología proporciona servicios varios como el intercambio electrónico de datos (EDI), el videotex, el correo electrónico, la transferencia electrónica de fondos (FTP) y el acceso a los bancos de datos, integrando una plataforma tecnológica que permite el tratamiento e intercambio de cantidades ilimitadas de datos de la más variada naturaleza. Éstos, a su vez, constituyen el insumo principal a partir de los cuales se origina la información, es decir, son precisamente el producto de su procesamiento o tratamiento y de su orientación a una finalidad determinada.

Ahora bien, la hoy llamada "***sociedad de la información***", también denominada "***digital***" o "***cibernética***", tiene como materia prima a la información que, como actividad y como bien, es la principal fuente de riqueza y principio de organización de la misma. (Cfr. Joyanes Aguilar, 1997:86). En la actualidad, empresas públicas, privadas y administraciones públicas invierten cuantiosas sumas en desarrollar sistemas de información automatizados que les permitan producir información para atender a sus requerimientos organizacionales y en consecuencia, intercambian y manipulan la más amplia variedad de datos, de diversa índole y con diferentes finalidades.

Por otra parte, las técnicas de la informática han permitido la creación de grandes bancos de datos, tanto públicos como privados, que almacenan enormes volúmenes de información, incluyendo los datos de carácter personal y que junto con la telemática, permiten el tratamiento de los mismos en el más amplio sentido de la palabra.

No obstante las bondades de los servicios telemáticos, muchos de ellos incorporados con gran éxito al *modus operandi* empresarial, éstos implican una serie de riesgos derivados de la facilidad del tratamiento de datos personales que pueden vulnerar algunos derechos fundamentales, principalmente el de la privacidad.

Entre los riesgos asociados con estas nuevas tecnologías se han señalado la creación de *perfiles* mediante el *entrecruzamiento de datos personales*, la *asignación de identificadores únicos* para toda la Administración Pública, la *etiquetación* y *categorización* de sujetos sin matices ni variantes, la *agregación de datos* y la *toma de decisiones* únicamente tomando como referencia la información contenida en los bancos de datos (informática decisional), entre otros. (1)

2.- La creación de grandes autopistas de la Información, como por ejemplo, Internet. Ëstas autopistas de la información como refiere Joyanes Aguilar "son el conjunto de medios físicos y de las informaciones que viajarán por ellos para permitir todo tipo de comunicaciones"(Op.cit.:156). Ellas constituyen las infraestructuras nacionales de información y presentan como característica principal que permiten la comunicación de grandes cantidades de datos, a muy alta velocidad , desde y a cualquier parte del mundo, sin restricciones de fronteras. Ahora bien, la red Internet, la más popular y grande de estas autopistas es conocida como la red de redes, con cobertura mundial que consta de millares de redes independientes en instalaciones académicas, militares, gubernamentales y comerciales. En Venezuela, esta red ha expandido su uso a finales de la década de 1990. Si bien en nuestro país, el número de usuarios (internautas) se ubica en trescientos cincuenta y siete mil (357.000) aproximadamente, para un total en América Latina de siete millones trescientos ochenta y nueve mil cuarenta y dos usuarios (7.389.042) (América Economía, 1999:64), la tendencia reflejada en los últimos años es al aumento progresivo de su utilización e incorporación de nuevos usuarios.

Ahora bien, en Internet circulan millones de datos de las más variada naturaleza. La World Wide Web aloja a numerosos sitios o establecimientos virtuales que obtienen información relativa a personas identificables. Se calcula que el noventa por ciento (90%) de los sitios comerciales de la Web obtienen información de esa naturaleza y apenas un catorce por ciento (14%) informan al usuario sobre la obtención de datos personales. Mientras que el ochenta y nueve por ciento (89%) de los Webs destinados al público infantil obtienen información personal de los visitantes, sólo un cincuenta y cuatro (54%) informan a los usuarios sobre dichas operaciones. (2)

Se evidencia pues una manipulación por parte de las empresas virtuales en la Web que obtienen información personal sin que la mayoría de ellas informen a los sujetos, cuál es el destino y la finalidad de la recolección de datos, aunado al hecho de que no ofrecen las garantías mínimas de su protección.

---

(1) Es por ello que algunos ordenamientos jurídicos han prohibido, incluso constitucionalmente, la asignación de un número único de identificación personal a los ciudadanos para usos universales o han previsto algunas garantías para evitar los riesgos anteriores. Así por ejemplo, en Francia el proyecto SAFARI que pretendía crear un identificador único para los ciudadanos en todas las relaciones con la Administración, fue rechazado categóricamente por los ciudadanos. Así mismo, la Ley francesa Informática y Libertades número 78-17, del 6 de enero de 1978, prevé como garantía la exclusión absoluta de los perfiles como base de las decisiones judiciales o base única de decisiones administrativas o privadas.
(2) Datos suministrados por el Informe FCT sobre marketing e intimidad en Internet, formato electrónico: http://www.onnet.es/03002004.htm

Ahora bien, la solución que el derecho ha aportado para asegurar la libertad del hombre ante las situaciones antes expuestas ha sido la configuración del derecho a la libertad informática y el derecho a la privacidad.

La libertad informática ha sido denominada por la doctrina española más calificada como *"un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas para: conocer y acceder a las informaciones que les conciernen archivados en bancos de datos (lo que se denominada habeas data por su función análoga en el ámbito de la libertad de información a cuanto supuso el tradicional habeas corpus en lo referente a la libertad personal), controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su tramisión"* (Pérez Luño, 1989:140)

De igual manera, la libertad informática forma parte del núcleo de derechos denominados de *"tercera generación"*, en los cuales se incluyen el derecho a la paz, los derechos de los consumidores, el derecho a un medio ambiente sano y el derecho a una calidad de vida, derechos éstos dirigidos a potenciar la esfera de libertades del individuo en la era tecnológica.

La libertad informática constituye además un elemento de legitimación política de los sistemas democráticos con avance tecnológico. Por otra parte, la libertad informática también puede ser entendida de acuerdo con lo que el Tribunal Constitucional Alemán ha calificado del ***"derecho a la autodeterminación informativa"***, en su célebre sentencia del 15 de diciembre de 1983, que declaró inconstitucionales algunas disposiciones de la Ley del Censo de la República Federal Alemana. En tal sentido, el mencionado Tribunal señaló que dicho derecho supone la facultad del individuo de disponer y revelar datos referentes a su vida privada. Asimismo, el derecho a la autodeterminación comporta para el individuo disponer sobre sus datos personales en ***"todas las fases de elaboración y uso de datos, o sea, su acumulación, su trasmisión, su modificación y su cancelación"***. (Ibid:140) No obstante, el derecho a la autodeterminación informativa encuentra como único límite admisible la existencia de un interés general superior.

Con esta orientación, la libertad informática es protegida mediante la consagración del derecho a la intimidad. Sobre este derecho, que en un comienzo la doctrina lo entendía como la facultad del individuo a estar solo (*rigth to be alone*), en la actualidad, según Adalbert Podlech, ***"la intimidad, más que un estado de autoconfinamiento supone una determinada calidad de la relación con otros"***. (Pérez Luño, op.cit:157).

De este modo, la doctrina y jurisprudencia española han trasladado el contenido esencial del derecho a la intimidad desde la facultad de aislamiento *(ius solitundinis)* al poder de control sobre las informaciones relevantes para cada sujeto. Se observa entonces una evolución positiva de este derecho configurado primigeniamente en sentido negativo.

De esta misma manera ha sido entendida por la jurisprudencia argentina. En efecto, la Corte Suprema de Justicia de la Nación señaló: *"en la era de las computadoras el derecho a la intimidad ya no puede reducirse a excluir a los terceros de la zona de reserva, sino que se traduce en la facultad del sujeto de controlar la información personal que de él figura en los registros, archivos y bancos de datos..."*(CNFed.Civil y Com, 1995)

Por otra parte, el derecho a la intimidad abarca un núcleo en el que se pueden encontrar ciertos derechos como: la protección al honor o dignidad, que trae como consecuencia la reparación del daño que produce la divulgación de la vida íntima; la protección del anonimato autoral como el caso de los seudónimos a fin de proteger la identidad individual y la protección del secreto, como por ejemplo del secreto profesional. (Cfr. Quiroga Lavié,1995:51)

Como fuese señalado anteriormente, el desarrollo vertiginoso de las nuevas tecnologías amenaza invadir espacios antes no conocidos de la intimidad personal, lo que hace perentorio profundizar el alcance del mencionado derecho. De allí que se pueda hablar de un derecho que regule y proteja la intimidad en materia de tratamiento de la información de índole personal, el cual ha sido denominado ***"derecho a la intimidad informática"***. Para algunos autores (Davara, Del Peso, Pérez Luño), se trata de proteger lo que la doctrina anglosajona denomina ***"privacy"***, término castellanizado como ***"privacidad"***, que le garantiza al ciudadano el derecho a exigir que permanezca en su esfera interna el resultado del tratamiento de su información personal.

La sustitución del término *"intimidad"* por *"privacidad"* ha sido acogida también por el legislador español. Al respecto, en la exposición de motivos de la Ley Orgánica Española de Regulación del tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) No. 5/1992, se señaló que: *"la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona...la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado...."*. *(subrayado nuestro)*

En consecuencia, las nuevas tecnologías de la información y la comunicación le añaden a la privacidad un elemento nuevo: *"la necesidad de proteger al individuo ante la posibilidad de que los datos que se contienen en archivos informáticos diversos, por tanto, fuera del espacio que la persona se mueve-pongan de manifiesto una personalidad determinada, cuyo conocimiento pueda decidir a los demás a tratarla de una manera perjudicial para sus intereses o, en todo caso, de una forma predeterminada" (De Carreras Serra, op.cit.:82)*

Se deduce entonces que la privacidad tiene una mayor fuerza expansiva que la intimidad. Mientras que esta última abarca la protección de la esfera en la cual la persona se desenvuelve, es el caso de su domicilio, comunicaciones privadas, la concepción más reciente de la privacidad elaborada por la doctrina (Maglio, 1999:14) engloba cuatro espacios específicos, a saber: (a) la soledad que es la manifestación más absoluta del fenómeno de la privacidad; b) la intimidad como una categoría intermedia de privacidad, c) el anonimato como la situación en la cual el individuo entra en contacto con otros sin identificarse en forma alguna y d) la reserva, que representa el último estadio de la privacidad y se realiza a través de la constitución de una barrera física o psicológica para proteger al individuo de intrusiones no deseadas. Vgr. Que se protega al individuo de crear perfiles de su personalidad a través del entrecruzamiento de datos.

En conclusión, la tutela de la privacidad posee una fuerza expansiva que le permite afirmarse como un instrumento general de protección de la persona en todas sus manifestaciones y facetas como sujeto que se coloca en relación con otros.

Ahora bien, la novísima Constitución Nacional de la República Bolivariana de Venezuela de 1999 consagró por primera vez en nuestra historia constitucional el derecho a la libertad informática, en el artículo 28, Capítulo I del Título III *"**De los deberes, derechos humanos y garantías, Disposiciones generales**"* en los siguientes términos:

> *"Toda persona tiene derecho de acceder a la información y a los datos que sobre si misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos. Igualmente podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes periodística y de otras profesiones que determine la ley".*

La anterior disposición consagra expresamente el *"**derecho a la libertad informática**"* por cuanto reconoce el derecho de cualquier individuo a conocer, controlar y disponer sobre sus datos personales que consten en archivos o registros oficiales y en los privados, previéndose asimismo otras facultades que forman parte del núcleo de derechos que implica la libertad informática, tales como: el derecho de información, en este caso, el derecho de los titulares de los datos a conocer la existencia del registro y de su finalidad; el derecho de acceso, es decir, al conocimiento de sus datos personales; el derecho de rectificar, de actualizar y de cancelar aquellos datos personales incompletos, desactualizados o inexactos o aquellos que afecten ilegítimamente sus derechos.

Por otra parte, se consagra que los derechos de control de la calidad de los datos personales, esto es, los derechos a la actualización, rectificación o cancelación, se ejerzan a través de la conocida figura del ***"Habeas Data"***, acción judicial que interpone el titular de los datos por ante los tribunales competentes respectivos para el ejercicio efectivo de los mismos.

En consecuencia, se observa en la novísima normativa constitucional venezolana la consagración expresa tanto del derecho a la libertad informática como de su garantía o tutela, con la acción de Habeas Data.

Se podrían indicar como aspectos favorables en la configuración del derecho a la libertad informática antes señalado, su reconocimiento expreso como un derecho fundamental, autónomo, inherente a la persona humana y de rango constitucional, así como el de su garantía para su tutela efectiva, lo cual supone un avance indiscutible en el proceso de positivización de los derechos que conforman la parte dogmática del texto constitucional, con lo cual nuestro constituyente se articula e inserta con la tendencia de las más recientes producciones constitucionales latinoamericanas y por otra parte se incluye uno de los más significativos "derechos humanos de tercera generación", como respuesta a las exigencias de libertad del hombre frente a las nuevas realidades tecnológicas.

Con relación al contenido esencial del derecho a la libertad informática, los derechos de acceso y control se extienden, como indica el artículo 28, a los datos personales contenidos en registros oficiales o privados, con las excepciones que establezca la ley. Ahora bien, el diseño normativo previsto en el artículo 28 en comento plantea al operador jurídico la interrogante sobre qué debe entenderse por "registros oficiales" y "privados", puesto que es a los datos personales contenidos en estos registros que el Constituyente otorga la protección constitucional. A nuestro juicio el Constituyente parece entender por registros oficiales aquellos archivos bajo la responsabilidad y *organización de la Administración Pública en sentido lato (central y descentralizada); y por registros privados*, aquellos organizados y dirigidos por personas de carácter privado, como podría ser el caso de las bases de datos administradas por los bancos comerciales y las empresas aseguradoras del sector privado.

De igual manera, acertadamente a nuestro entender, no se hace mención a la condición de que los datos personales se encuentren en archivos o registros automatizados, con lo cual se deja la posibilidad de otorgar protección a los datos personales contenidos en archivos públicos o privados con carácter público, no automatizados; es decir, la tutela se otorga independientemente de que los datos se encuentren contenidos en soportes informáticos y con la previsión anterior, se recoge la tendencia de la protección europea de la libertad informática en el sentido que la tutela se otorga sin tomar en cuenta la modalidad que pueda revestir el almacenamiento de los datos personales.

Por otra parte, se observa del análisis del Habeas Data propuesto, su amplitud de redacción, dado que se pueden ejercer los derechos de control de la calidad de los datos personales, esto es, los derechos de actualización, rectificación y cancelación frente a diversas hipótesis normativa tales como: datos incompletos, inexactos, desactualizados o ilegítimos; o cuando dichos datos aún siendo completos o actualizados, afecten de cualquier manera ilegítimamente los derechos de sus titulares.

*En cuanto a los requisitos de fondo y de forma para interponer y admitir la acción de "**Habeas Data**" ante los* Tribunales competentes así como del resto del procedimiento judicial, el Constituyente omitió reservar expresamente todos estos aspectos a la Ley, lo cual no obsta a que se pueda afirmar que sobre el mismo existe el principio de reserva legal, puesto que una de las garantías de los derechos fundamentales estriba precisamente en que el desarrollo de su contenido esencial está reservado al legislador, de conformidad con lo previsto en el artículo 156 de la Constitución que establece como competencia exclusiva del Poder Público Nacional la legislación sobre los derechos, deberes y garantías constitucionales. Asimismo, esto constituye un principio de protección del contenido esencial de los derechos fundamentales.

En otro orden de ideas, consideramos que para que el recurso de Habeas Data pueda lograr sus fines, es decir, garantizar el ejercicio efectivo de los derechos de la libertad informática, en la configuración posterior del procedimiento que realizará el legislador, éste deberá tener como norte los principios de sencillez, transparencia, economía y celeridad procesal de tal manera que constituya un mecanismo eficaz que permita al individuo el acceso fácil, expedito y económico a sus datos personales, puesto que de no ser así se desnaturalizaría la ratio legis de dicha garantía al impedir su realización práctica.

De igual forma, observamos como limitante en el diseño normativo de la disposición 28 del mencionado Proyecto Constitucional, el establecer el "Habeas Data" como único mecanismo de tutela de la libertad informática. Hubiera sido preferible una redacción que contemplara también la tutela administrativa, de tal manera de re-

solver las pretensiones dirigidas a hacer efectiva la libertad informática en un primer momento ante los órganos administrativos y en un segundo momento, ante los jurisdiccionales, en caso de apelación de las decisiones formuladas por los primeros.

Asimismo, el análisis de la cláusula del artículo 28 se debe articular con el contenido del artículo 60 de la Carta Magna que establece textualmente: ***"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos."***.

Esta disposición guarda estrecha vinculación con el derecho a la libertad informática y al habeas data, puesto que refiere los distintos aspectos de la vida privada del individuo merecedores de tutela jurídica y como ha sido señalado en este trabajo el derecho a la libertad informática se encuentra garantizado a través de los derechos a la intimidad y a la privacidad informática.

En este sentido, la cláusula contenida en el artículo 60 presenta como aspectos resaltantes y favorables la diferenciación de las distintas facetas individuales tales como la imagen y la intimidad, lo cual evidencia la ampliación de la esfera de la protección a la vida privada, diferenciándose claramente entre "***vida privada***" e "***intimidad***", lo cual no es más que el reconocimiento expreso de los ámbitos de lo íntimo y de lo privado, redacción que reafirma la tesis planteada en el presente estudio. Asimismo, con esta disposición el Constituyente sigue el modelo de las constituciones de Brasil y Perú, en las cuales también se distinguen nítidamente estos dos espacios fundamentales de lo individual.

Ahora bien, hubiese sido deseable incluir en el referido artículo 60, dentro de la protección a la vida privada otras facetas personales tales como el derecho a la voz y a la intimidad familiar, con una redacción mucho más amplia y abierta a otros "aspectos o caracteres que contribuyan a la identificación personal" puesto que en esta materia, en la medida en que evolucionan las tecnologías y la sociedad, se manifiesta una tendencia a la necesidad de proteger otros espacios individuales, previsibles o no y que puedan ser amenazados por el uso de las nuevas tecnologías.

Con respecto a la protección de la vida privada, como antes se indicó, está suficientemente garantizada en el artículo 60 ya señalado y encontramos en la trayectoria constitucional venezolana antecedentes varios de su protección, tal como la otorgada por la Carta Magna del 61 que establecía en su artículo 59 el derecho de toda persona a ser protegida contra intrusiones o invasiones a su vida privada. Posteriormente, en el desarrollo legislativo de la referida disposición fundamental, el legislador patrio en 1991 sancionó la Ley sobre Protección a la Privacidad de las Comunicaciones con el fin de proteger "*la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas*" (Artículo 1). Y a nuestro entender, la protección de la mencionada ley es aplicable de igual forma a las comunicaciones realizadas a través de las nuevas tecnologías de la información y comunicación. Vgr. Internet.

Por otra parte, la jurisprudencia venezolana también ha reconocido expresamente "***el derecho a la privacidad***", como un derecho fundamental de todo individuo. En la sentencia de fecha 14/08/88, que resuelve el recurso de amparo incoado por enfermos de VIH/SIDA contra el Ministro de Sanidad y Asistencia Social, la Corte Suprema de Justicia acordó el carácter reservado de las actuaciones de la misma, a petición de los demandantes (enfermos de sida), a fin de proteger su identidad y evitarles posibles estigmatizaciones o el escarnio público.

Se observa entonces una evolución del derecho a la privacidad en el ordenamiento jurídico venezolano y en el derecho comparado, que se manifiesta en una tendencia a que en éste confluyan a su vez un conjunto más amplio de espacios de lo individual merecedores de tutela jurídica. Podriamos concluir que es la facultad de todo individuo a construir libremente su vida privada o espacio vital y a rechazar cualquier forma de injerencia o control público o social, en un ámbito calificado de libertades para las escogencias fundamentales de la vida.

LA LIBERTAD INFORMATICA EN EL DERECHO COMPARADO

A continuación se presenta cuadro comparativo de las disposiciones fundamentales sobre la libertad informática y los derechos a la intimidad personal y familiar y a la privacidad en las Constituciones de América Latina

PAÍS	Art.	CONTENIDO DEL ARTÍCULO
ARGENTINA	**43**	**Artículo 43o.-** Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial mas idóneo, contra todo acto u omisión de autoridades publicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva. Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminacion, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística. Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o, en caso de agravamiento ilegitimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de habeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio.
BRASIL	**5/10 22/IV 102/d**	**Artículo 5o.** Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el País la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los siguientes términos: ...**10**: . son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación.... **Artículo 22.** Compete privativamente a la Unión legislar sobre:...**IV:** aguas, energía, informática, telecomunicaciones y radiodifusión;... **Artículo 102.** Es competencia del Supremo Tribunal Federal, principalmente, la garantía de la Constitución, correspondiéndole: I. procesar y juzgar, originariamente: ....**d)** los habeas corpus, siendo sujeto pasivo cualquiera de las personas señaladas en las líneas anteriores; los mandados de segurança y los habeas data contra actos del Presidente de la República, de las Mesas de la Cámara de los

		Diputados y del Senado Federal, del Tribunal de Cuentas de la Unión, del Procurador General de la República y del propio Supremo Tribunal Federal;....
CHILE	**19/4**	**Artículo 19**. La Constitución asegura a todas las personas:.... **4º** El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia. La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan; ....
COLOMBIA	**15**	**Artículo 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.
ECUADOR	**23/8** **23/12** **23/13**	**Artículo 23**.- Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: 8.**El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona.** **12.**La inviolabilidad de domicilio. Nadie podrá ingresar en él ni realizar inspecciones o registros sin la autorización de la persona que lo habita o sin orden judicial, en los casos y forma que establece la ley. **13**.La inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación.
HONDURAS	**76**	**Artículo 76.** Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen.

MÉJICO	**16**	**Artículo 16.** Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. ... Las intervenciones autorizadas se ajustaran a los requisitos y limites previstos en las leyes. Los resultados de las intervenciónes que no cumplan con estos, careceran de todo valor probatorio. La autoridad administrativa podrá practicar visitas domiciliarias unicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policia; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetandose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos. En tiempo de paz ningún miembro del ejercito podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento, bagajes, alimentos y otras prestaciones, en los terminos que establezca la ley marcial correspondiente.
NICARAGUA	**26**	**Artículo 26.-** Toda persona tiene derecho: 1.A su vida privada y la de su familia. 2.A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. 3.Al respeto de su honra y reputación. 4.A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información....
PARAGUAY	**135**	**Artículo 135.** Toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos si fuesen erróneos o afectaran ilegítimamente sus derechos.
PERÚ	**2/4** **2/6** **2/7** **2/10**	**Artículo 2º** Toda persona tiene derecho:.... **4.** A las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley....**6.** A que lo servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. **7.** Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. ...**10.** Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados....

LISTA DE REFERENCIAS

AMÉRICA ECONOMÍA (1999) Públicación Número 158 del 20 de mayo de 1999.

BADENI, Gregorio (1994) Reforma Constitucional e Instituciones Políticas**. Buenos Aires.**

DE CARRERAS SERRA, Lluís. (1996) Régimen jurídico de la Información. Periodistas y medios de comunicación. **Barcelona, Editorial Ariel.**

JOYANES AGUILAR, Luis (1997). Cibersociedad: la nueva sociedad de la información. (Orígenes, evolución e implantación). En**: Sociedad y Utopía.** Revista de Ciencias Sociales. Informática y Sociedad. Facultad de C.C.P.P. y Sociología León XIII. Fundación Pablo VI. No. 9.

MAGLIO, Marco. (1999) **La Tutela dei Dati Personali**. Napoli, Edizioni Giuridiche Simone.

PEREZ LUÑO, Antonio Enrique (1989). Los derechos humanos en la sociedad tecnológica. En **Cuadernos y debates**. No. 21 centro de Estudios Constitucionales. Madrid.

QUIROGA LAVIÉ, Humberto (1995) **Los derechos humanos y su defensa ante la Justicia.** Bogotá, Editorial Temis.

Contratación electrónica, comercio electrónico, firma digital: Planteamientos y alternativas de solución

Vania Vergara Lau / Luis Quiñones Olivo (Perú)
Estudiantes Universidad Privada del Norte. Trujillo - Perú

1. CONTRATACION ELECTRONICA.

1.1. Introducción:

1.2. Concepto:

Es la declaración conjunta de la voluntad común de dos o más partes expresada a través de medios electrónicos, la cual genera obligaciones recíprocas lícitas de carácter patrimonial.

1.3. Naturaleza Jurídica:

Sería ilógico referirse a la naturaleza jurídica de los contratos electrónicos, pues éstos revisten múltiples modalidades. Esta complejidad contractual surge por las necesidades de las partes contratantes sin considerar fronteras físicas o de envergadura; es decir, que una gran corporación puede recurrir a artesanos por servicios particulares o viceversa, sin importar su localización geográfica, o lengua de comunicación.

1.4. Características:

Los contratos electrónicos presentan caracteres jurídicos propios de todos los contratos, los cuales se presentan según los modos de contratación entre las partes. Así, podemos señalar las siguientes características:

a) Consensualidad.- Por regla general, los contratos electrónicos son consensuales ya que se perfeccionan sin necesidad de ninguna formalidad; pero no se puede descartar los casos donde se requiere exigir la literalidad, característica que debe ser impuesta por normas jurídicas internacionales, pues sería erróneo considerar que la literalidad se ajuste a leyes de un determinado país o una determinada jurisdicción, porque los contratos electrónicos, no son más que contratos efectuados dentro de una gran aldea, como su fuera una gran nación, y por tanto se debe de regir por reglas generales, sencillas y prácticas que permitan su desarrollo de manera dinámica.

b) Autónomo.- De acuerdo con esta característica, podemos afirmar que los contratos electrónicos serán autónomos cuando así lo sea el negocio de que se trate, en razón que no se puede descartar que se configuren bajo las formas de contratos accesorios y derivados.

c) Tipicidad.- Existen muchas posiciones al respecto, pero consideramos que los contratos electrónicos no pueden clasificarse estrictamente en típicos y atípicos, pues ello dependerá del tipo de negocio de que se trate y de las necesidades de las partes intervinientes en la contratación. En consecuencia, tampoco se puede descartar la existencia y desarrollo de contratos híbridos.

d) Onerosidad.- Los contratos electrónicos por lo general se celebran a título oneroso; es decir, cada una de las partes tiene a su cargo una prestación, tal como sucede con los contratos de compraventa, arrendamiento, entre otros que se realizan comúnmente por medios electrónicos. Sin embargo, no existe inconveniente alguno para la celebración de contratos a título gratuito, pues aunque no sea usual, podría darse de común acuerdo de las partes.

e) Conmutatividad.- En la actualidad, los contratos electrónicos se han extendido por el criterio de riesgo hasta aleatorios, tal como se aprecia en aquellos contratos de juegos y azar a los que se puede ingresar por medios electrónicos como Internet. Por otro lado, no se puede dejar de resaltar que son los contratos de característica conmutativa los más populares y frecuentes para la realización de transacciones comerciales de todo tipo de magnitud.

f) Reciprocidad de prestaciones.- Los contratos electrónicos en su mayoría son de prestaciones recíprocas, pues la prestación de una de las partes está sujeta a una contraprestación de la otra parte. Sin embargo, como hemos afirmado en los numerales anteriores, no podemos limitar su extensión y complejidad; en este sentido, podemos afirmar que los contratos electrónicos pueden ser con prestación unilateral, tal como se da con el servicio de correo electrónico que brindan algunas entidades en Internet, o también con las donaciones de programas (globalink, antivirus, etc.), entre otros.

g) De ejecución inmediata o de tracto sucesivo.- Los contratos electrónicos, por su compleja naturaleza, surten efectos que pueden ser de ejecución inmediata, diferida, de tracto sucesivo, a plazo fijo y a plazo indeterminados.

1.5. Modalidades:

En la actualidad, los contratos electrónicos se desarrollan por toda una gama de medios tecnológicos, como lo son los medios fonográficos, tales como el Telebanco, Telemercado, etc.; los medios digitales, el Internet; los e-mails; el IRC; el ICQ; el fax y otros documentos electrónicos.

En las contrataciones electrónicas, las necesidades de conocer físicamente a la contraparte no son fundamentales, se requiere que las partes confíen entre sí. Aquí se destaca que, las envergaduras o magnitudes de las empresas no difieren entre sí, pues lo importante es que éstas sean competentes. En consecuencia, la relación comercial se vuelve una relación más estrecha entre las partes que negocian; en virtud de algunas modalidades de negociación.

Esta dinámica de las contrataciones electrónicas genera que las empresas se vuelvan más personalizadas y en otros casos de negociación masiva con solo "un clic"; en razón de las vertiginosas velocidades con las que reducen los costos y minimizan las distancias y fronteras de lengua y cultura.

En virtud de las ventajas tecnológicas que se nos brinda, el comercio electrónico tiene la facultad de poder manejar simultáneamente una serie de proveedores y potenciales alternativas, así como el llegar a un sin fin de clientes en tiempos realmente asombrosos. Ello produce una lucha desmedida por no perder un cliente en la red, desencadenando en una confrontación voraz entre grandes corporaciones y pequeños productores donde la creatividad y habilidad para el negocio sean los factores decisivos, prevaleciendo sobre la capacidad de recursos.

En este nuevo mercado las empresas tienen la facilidad de crecer sin establecer una infraestructura física grande o estable, sino que sólo basta con ser eficientes a la hora de cubrir las necesidades del consumidor.

El continuo uso de transacciones comerciales electrónicas generan una dependencia hacia el computador y por consiguiente, se puede establecer el nacimiento de una nueva generación de consumidores y comerciantes, los cuales no encajan en ningún sistema ya establecido dado que las diversidad de necesidades y de ofertas lo hace ser el mercado más económico y dinámico que se pueda haber generado.

De esta manera, surge la marca, como una forma de sustentar y acreditar la individualidad y personalidad de un producto, volviéndose una herramienta fundamental. Asimismo, otro elemento indispensable es el canal de distribución, el cual encuentra un solo limitante que son las fronteras y jurisdicciones geográficas. Pero, la creatividad que este nuevo sistema fomenta de manera vertiginosa, nos permite que podamos hacer uso de los distintos medios

ya existente o de crear los que sean necesarios, en muchos casos éstos son más veloces que los ya conocidos y cubren distancias que antes no podríamos cubrir al costo actual.

1.6. Elementos:

1.6.1. De las partes.- Las partes intervinientes en los contratos electrónicos pueden ser una o más personas, que actúen de manera individual, colectiva u organizada en personas jurídicas.

Por su extensión, los contratos electrónicos pueden ser abiertos o restringidos, según el objeto de la prestación, pues el objeto se puede restringir por la moral, las buenas costumbres o la ética.

a) Impedimentos.- Podemos concebir como causales de impedimento de participación en las relaciones contractuales el atentar contra la dignidad, moral, buenas costumbres o ética de las personas. Asimismo, es causal de impedimento el incumplimiento de obligaciones adquiridas dentro de la red, el cual se sancionará con la restricción de participación influyente dentro de la red, dejándolo sólo como receptor.

b) Capacidad e Incapacidad.- Siguiendo el sentido de la concepción de la intervención de las partes contratantes, la capacidad de éstos será según el tipo de negocio que se celebre. De esta manera, será abierto para el intercambio de productos y prestación de servicios de todo tipo para las personas moral, física y síquicamente aptas; respetando las buenas costumbres y la ética de la aldea.

c) Derechos y Obligaciones.- Surgen de acuerdo a las necesidades y negociaciones que efectúen las partes contratantes, respetando y cumpliendo todas las prestaciones a las cuales se han obligado consensualmente.

1.6.2. El Objeto de la Prestación.- El objeto de la prestación del contrato electrónico comprende a cualquier objeto tangible e intangible, o cualquier objeto que pueda ser recepcionado por las partes que pueda ser percibido por cualquiera de los sentidos e incluso, puede ser cualquier el resultado de un producto derivado de la siquis de una persona.

1.7. Efectos:

Los contratos electrónicos producen efectos entre las partes por cuanto se han obligado en sus prestaciones acordadas.

Se resalta que el incumplimiento de las obligaciones generadas por el contrato electrónico, produciría el bloqueo de acceso de participación influyente dentro de la red; es decir, que toda participación como emisor tendrá una notificación impuesta de página u opinión restringida. Esta notificación será insertada por los organismos o entidades certificadoras del incumplimiento de las obligaciones del deudor.

1.8. Resolución de Controversias y conflictos:

Ante el surgimiento de controversias y conflictos entre las partes contratantes, éstos podrían recurrir a las entidades u organismos especializados en la resolución de conflictos de la naturaleza del contrato; es decir, los medios alternativos como el arbitraje, la conciliación, y la mediación funcionarían en la red de manera institucional, con especialidades en diversas materias y conformado con especialistas de la materia, tales como los profesionales, técnicos o conocedor de la temática del conflicto referente a la realidad que refleja la aldea.

2. COMERCIO ELECTRONICO.

2.1. Descripción:

El comercio electrónico en el principio de agilizar, muestra una diversificación de productos, pluralidad de proveedores; siendo su extraordinaria cualidad la de estrechar distancias y localizar más rápido los productos a nivel del globo.

2.2. Medios de Pago:

Los medios de pago no son limitados por las fronteras ni entes financieros tradicionales, sino que a manera de cómo evoluciona el comercio, así mismo evolucionan las formas de pago; en este caso, podemos mencionar desde las tarjetas de crédito, hasta las transferencias de cuenta a cuenta, pasando por pagos al contado, etc.

2.2.1. Sistemas de Pago.- Los sistemas de pago pueden diversificarse de acuerdo al medio geográfico o magnitud de la transacción. En el primer caso, podemos establecer como medio internacional para productos de pequeña y mediana envergadura a la tarjeta de crédito como la más frecuentada.

Otro sistema de pago sería a través de cartas fianzas, warrants, y demás herramientas de comercio internacional.
Pero, donde mayor desarrollo y creatividad se genera, es en el pago en zonas locales donde se puede establecer desde créditos en línea hasta cobros a contra entrega ya que el riesgo es disminuido debido al conocimiento del cliente.

En sistemas locales, en especial Latinoamérica, donde las economías no son del todo sólidas y estables, podemos proporcionar al cliente un sistema de pre-pago, lo que significaría comprar dinero para usar en Internet. La aplicación de este sistema sería de la siguiente manera:

En un primer lugar, el cliente adquiere una tarjeta por un monto ya fijado, teniendo capacidad de crédito por dicho monto, ya que esta tarjeta generará un crédito en una tarjeta o cuenta bancaria internacional, por medio de la cual tendrá acceso al consumo en la red sin restricción de procedencia de los ofertantes. Para los ofertantes, esto incrementaría sus precios de venta en un porcentaje no mayor del porcentaje que se incrementaría su consumo.

En transacciones de magnitudes significativas, la tasa tendría un porcentaje preferencial y la adquisición de las mismas ya no sería de manera tan ambulatoria, sino que recurriría a un establecimiento de confianza que brinde la seguridad del caso.

Por otro lado, en las economías desarrolladas generaría un nuevo cliente, el cual estaría segmentado entre menores de edad con acceso restringido a tarjetas de crédito o herramientas similares y a su vez permitiría un control del consumo para quienes lo deseen.

2.2.2. Seguridad.- La seguridad que se otorga en los sistemas de pago de comercio electrónico se sustenta en la no existencia de capacidad de endeudamiento, en razón de que el consumo es efectuado por adelantado. Cabe resaltar, que para las empresas tanto que oferten como que consuman se verán beneficiadas al obtener una economía dinámica y una tasa de retorno similar.

a) Criptografía.- La codificación se basaría en una serie de números aleatorios generados bajo ciertos comandos, los cuales mutarían cada cierto tiempo; con lo que tendríamos una seguridad más sólida respecto al ocultamiento y privacidad tanto de documentos, códigos, accesos, correos y demás información de carácter personal.

2.2.3. Organismos Reguladores.- La regulación estaría dada de acuerdo a una clasificación basada en las magnitudes de las transacciones; por ejemplo, para transacciones menores sólo bastaría con el ente

generador del dinero electrónico, más para transacciones medias o importantes se recurrirían a herramientas financieras del comercio internacional, según sea el caso.

Estas entidades sólo intervendrían en el plano financiero, más en el plano legal o moral se recurriría a peritos técnico-profesionales y con fe de moralidad y ética, sin importar la procedencia o nacionalidad de los mismos, más sí su representatividad en la red.

Todo esto se organizará en una especie de Instituciones Conciliadoras o Arbitrales en las cuales no regiría nacionalidad alguna ni profesión, sino la capacidad técnico, moral y ético del individuo ante esta sociedad. La edad no sería una barrera de intervención, sólo sería necesario el probar la capacidad moral, ética y técnica de la persona como profesional en la red.

La certificación de estas personas se establecería en una reunión mixta entre profesionales legales de la sociedad tangible, tales como los notarios y fedatarios; y profesionales morales de la sociedad virtual, tales como las autoridades certificantes y los organismos fedatarios o reguladores.

Consideramos imprudente la intervención pura de personas vinculadas sólo a la normatividad en la sociedad tangible, *pero no imposible; dado que los requerimientos en conocimientos técnicos es tan importante como en* conocimientos legales.

3. FIRMA DIGITAL.

3.1. Definición:

La firma digital es la encriptación de una serie de datos personales y no duplicables los cuales poseerán dos passwords, el primero de ellos permitirá que el usuario pueda identificar la identidad del emisor y el segundo, que permita establecer la legalidad de dicha firma.

Para la generación de dicha firma se puede acceder por medio de un ejecutable, el cual llevaría a la visualización de un documento y a su vez de la firma digital, más no a la capacidad de edición de dicho documento o firma.

La única entidad capaz de modificaciones sería un notario; más la edición y generación del documento estaría en libre acceso para ambas partes sin limitante alguno.

3.2. Características:

La firma digital, a nuestro criterio, no debería contener la rúbrica, sino que contendría diversa información de carácter personal.

Sirve como una firma convencional, pero ésta es mucho más completa porque contiene como información *una fotografía de la persona, su ADN, grupo sanguíneo, DNI y su Huella Dactilar.*

3.3. Medios:

Los medios pueden ser diversos ya que éstos pueden ser transferibles como un todo; es decir como un ejecutable o como un documento u archivo con el cual sólo se pueda visualizar a fin de evitar adulteración alguna, esto significa que sería encriptado por una serie de passwords.

Nota: A efectos de la exposición, se ha diseñado un demo de firma digital, según nuestros planteamientos.

La Responsabilidad en el marco de la Actividad Informática**

Autora: Prof. Gladys Stella Rodríguez* (Venezuela)

INTRODUCCION.

En el presente trabajo se pretende determinar qué debe entenderse como riesgo siendo un presupuesto necesario para la responsabilidad, asimismo, determinar cuál es la noción de responsabilidad civil legal y sus alcances, describir la responsabilidad en las empresas informáticas, desde sus diferentes perspectivas, analizar el papel que juega la responsabilidad como institución jurídica en el marco de la actividad informática, desde determinar quienes participan en el proceso de negociación de la tecnología informática hasta determinar cuándo existe responsabilidad de parte del fabricante de equipos y sistemas informáticos.

La responsabilidad se encuentra consagrada desde tiempos remotos, pasando por una evolución significativa que parte de la época de la "venganza" que se mantuvo por mucho tiempo, trayendo la arbitrariedad, lo que hizo necesario la intervención del Estado para que actuara como un organismo regulador entre las comunidades participando como conciliador entre los litigantes y creando leyes para hacer más armonica la vida en comunidad; y así, se llega a las denominadas *amicabilis compositio,* que consistían en que aquella persona a quien se le causaba un daño recibía una indemnización en bienes destinada a reparar el daño. Desde aquella ley del talión, sin embargo, se fueron dando cambios y surgieron nuevas instituciones, como: la Ley de la XII Tablas y la Ley Aquilia, marcados esfuerzos para el nacimiento de la responsabilidad civil y penal de la sociedad actual

Sin embargo, en materia informática es necesario, dado que el progreso en la ciencia y la tecnología circula a un ritmo acelerado e inalcanzable, hacer una referencia aún que breve del alcance de la Responsabilidad por daños informáticos, máxime cuando no se puede ignorar las nuevas tendencias en el derecho de daños. Así, es oportuno considerar el grado de la responsabilidad de quien realiza una actividad informática o telemática, y la posibilidad de ejercer acciones por parte del usuario, quien se sirve de las posibilidades que brinda el intercambio de datos vía electrónica y la contratación informática en un mercado tan abierto como Internet. De allí la importancia del tratamiento de estos temas, a fin de crear criterios objetivos en el entendimiento que quien provoque una situación de riesgo debe – en principio – resarcir el daño que haya provocado.

1. SOCIEDAD DE RIESGO COMO PRESUPUESTO PARA LA RESPONSABILIDAD.

La historia de las relaciones entre técnica y Derecho es, la historia de un progresivo y creciente distanciamiento. El Derecho efectivamente se desconecta del desarrollo tecnológico cuando éste adquiere un ritmo vertiginoso y se desenvuelve en sectores cada vez más especializados. No obstante, llega un momento en que ese progreso técnico no puede ser en absoluto indiferente para el Derecho, que necesariamente se plantea entonces recuperar el control sobre las técnicas. No se trata de un dominio absoluto, pero sí de ejercer un control estratégico.

Precisamente, el momento de ejercer ese control se produce cuando la técnica genera riesgos. No se trata de que el Derecho no puede mantenerse indiferente ante el riesgo, sino que éste, el riesgo, incide decisivamente en la configuración del sistema jurídico hasta el punto de que algunas de sus más significativas inflexiones están marcadas por la idea del riesgo.

El concepto central de riesgo, por lo general se obtiene, por contraposición al de peligro. El peligro tiene causas naturales (enfermedades, catástrofes de la naturaleza, etc.) y, por ello, día a día el hombre hace esfuerzos por dominar a la naturaleza, según Ortega y Gasset, en ese proceso de reforma de la naturaleza en el que la técnica

(*)Doctora en Derecho. Magister en Planificación y Gerencia de Ciencia y Tecnología. Profesora e Investigadora de la Sección de Informática Jurídica y Derecho Informático del Instituto de Filosofía del Derecho "Dr. J.M. Delgados Ocando " e Internacional Público de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia - Venezuela.
(**) Avance del Proyecto de Investigación. Financiado por el Consejo de Desarrollo Científico y Humanístico (CONDES)

participa, se generan unos riesgos que ya no son los peligros de la naturaleza misma, producto de la técnica, sino los que precisamente ésta última origina, y que pueden denominarse "riesgos tecnológicos". Se trata, por tanto, de riesgos que no tienen un origen natural ajeno a la intervención humana, sino que se deben precisamente a la acción del hombre que va precedida así de una decisión, una decisión que como tal cuenta, con un estado de conciencia sobre los efectos posibles. Es entonces, en este grado de concientización que involucra toda decisión humana, lo que diferencia al riesgo del peligro.

Desde el punto de vista jurídico, se denomina riesgo o peligro a la situación jurídica que se presenta cuando las partes de un contrato, o de una de ellas, se encuentra en la imposibilidad de cumplir sus obligaciones o sus prestaciones debido a una causa extraña que no le es imputable (Maduro, 1967: 521). En este sentido, el concepto implica una conducta humana, es decir, una persona sea física o jurídica incumplen el acuerdo, sin embargo, la causa de ese incumplimiento no es imputable a esa persona. De allí, que desde el momento en que se habla de riesgos debido a la acción humana, su tratamiento jurídico es una cuestión ineludible al ser el objeto del Derecho la conducta humana y las relaciones sociales. Cuando esta actividad humana genera riesgos que lo son por su capacidad para producir daños, entonces parece que es la responsabilidad la institución adecuada para el tratamiento jurídico del riesgo. Así lo entiende Nieto (1994), al considerar primero, cómo "a medida que la sociedad se va complicando tecnológicamente, se convierte en forma progresiva en una sociedad de riesgo", para destacar seguidamente que "la sede natural del riesgo es la responsabilidad". Esto es y ha sido efectivamente así: es el régimen de la responsabilidad civil el que primeramente incorpora la idea de riesgo, y que decisivamente caracteriza, es que el riesgo traspasa el marco de la responsabilidad civil y su genuina funcionalidad reparadora para convertirse en un problema de Estado.

2.- RESPONSABILIDAD CIVIL: NOCION Y ALCANCES.

La responsabilidad civil es, la que en un primer momento se muestra sensible a la existencia de situaciones de riesgo cuya consideración altera sustancialmente las reglas. La responsabilidad originariamente concebida sobre la exigencia de culpa, responsabilidad subjetiva, pasa a configurarse con carácter objetivo, haciendo abstracción de la concurrencia de la culpabilidad: quien crea una situación de riesgo ha de responder objetivamente de los daños que de ella pudiera derivarse. Esa evolución de la responsabilidad civil discurre ya en paralelo al progreso tecnológico pues repara, precisamente, en los riesgos que comporta. En una sociedad poco desarrollada es necesario actuar dolosamente o con total negligencia para poder causar daños con un carro de bueyes. En una sociedad con cierto desarrollo tecnológico no es necesario una actuación negligente o dolosa para que puedan producirse graves daños con un vehículo cuyo motor es de inyección.

En cualquier caso, la responsabilidad civil, que altera de este modo sus criterios ante las situaciones de riesgo, mantiene su característica orientación reparadora (la solución que arbitra es el resarcimiento), aunque en los supuestos en que se establece la responsabilidad objetiva se abre una dimensión preventiva: quien se sabe responsable por los riesgos que genera, tratará en lo posible de reducirlos o evitarlos.

Este régimen de responsabilidad objetiva derivado de las situaciones de riesgo no es una novedad y opera ya desde hace un buen tiempo en el marco de relaciones perfectamente definibles atendiendo tanto a su elemento subjetivo (agentes y víctimas), como su conexión causal o a la limitación de sus efectos.(Pardo, 1999)

La noción de responsabilidad civil – entonces - radica en una concepción de derecho natural conocida desde muy antiguo y que sirve de norma fundamental de la vida del hombre en sociedad: la de que nadie puede causar un daño injusto a otra persona, y en caso de causarlo, dicho daño debe ser reparado. Siendo una situación evidentemente de carácter patrimonial resulta acertada la definición de Von Thur cuando afirma que la responsabilidad civil es la "situación jurídica del patrimonio de la persona que ha causado un daño injusto, quien queda obligado a repararlo".

Savatier, por su parte define la responsabilidad civil como "la obligación que incumbe a una persona de reparar el daño causado a otra por su propio hecho, o por el hecho de las personas o cosas dependientes de ella".

UNIVERSIDAD
LIMA

Tradicionalmente la doctrina distingue dos grandes categorías de responsabilidad civil: la contractual, que comprende el régimen de la indemnización de los daños y perjuicios causados por el incumplimiento culposo de una obligación derivada de un contrato; y la extracontractual, que comprende el régimen de la indemnización de los daños y perjuicios causados por el incumplimiento culposo de una obligación o de una conducta preexistente que no se deriva de ningún contrato. Sin embargo, la doctrina moderna, se inclina por una nueva estructuración de la responsabilidad civil, en el sentido de entender por ésta una única noción, una sola figura, una misma concepción con algunas derivaciones o efectos particulares integrados por la responsabilidad contractual y extracontractual.

La Actividad Informática: Un elemento a considerar

Se bebe considerar, y así lo ha hecho la doctrina prevaleciente en Italia, que distingue entre "peligrosidad de la conducta" y "peligrosidad de la actividad en sí misma considerada". Mientras la peligrosidad de la conducta se incluye en una categoría en la cual domina la culpa, la actividad peligrosa se inserta en otra categoría en la cual el núcleo está determinado por el elemento objetivo de la actividad misma, que es peligrosa en sí o por la naturaleza de los medios que adopta.

El concepto de actividad peligrosa es por su naturaleza un concepto relativo y depende del estado de avance de la ciencia y de la técnica en un sector determinado; lo que lleva a calificar de peligrosas a actividades que antes no lo eran o viceversa. De allí, que surja la inquietud acerca de considerar o no a la Informática, disciplina derivada del progreso tecnológico que hoy impera en las sociedades tecnológicas, como actividad peligrosa.

La multiplicidad de campos a los cuales se aplica, la necesaria automaticidad de los procesos en que interviene, la natural aptitud de pensar daños de toda índole (contractuales, extracontractuales, a bienes a personas, etc.), convierte a esta actividad en potencialmente peligrosa. Y por su puesto, el tema no deja de preocupar a la doctrina italiana, que encuentra en su Código Civil una base muy importante para el tratamiento de la responsabilidad civil derivada de actividades peligrosas.

Busnelli (1986), refiriéndose a la actividad vinculada con el software, hace referencia a la citada norma. Es verdad, que la jurisprudencia es bastante cauta en la aplicación de dicha regla, aun cuando ya es principio pacífico que actividades peligrosas no son solo aquellas previstas como tales en el texto ordenado de leyes de seguridad pública o en otras leyes especiales. Existen actividades que si bien no presentan como característica típica el requisito de peligrosidad, pueden volverse peligrosas si se las desarrolla de cierto modo, mientras que no lo son cuando se las ejerce en forma o modo distinto. Y éste, reafirma el autor, podría ser precisamente el caso de las actividades conectadas con la realización de un programa, las cuales en abstracto no son peligrosas, pero podrían convertirse en tales en concreto con relación a la específica operación a que se las refiere.

Tal vez una consideración genérica de la actividad informática es que las situaciones que pueden presentarse son de distinta magnitud, y ello naturalmente puede generar soluciones distintas. La amplitud misma de esta actividad puede provocar daños a terceros por fallas atribuidas al hardware, al software, a la gestión de bancos de datos, etc. En materia de bancos de datos pareciera que no existen disidencias en doctrina sobre la ubicación de tal actividad en la órbita de las actividades peligrosas. En cambio, podrían plantearse en lo atinente al hardware y al software. La producción de software para el desarrollo de actividades que pueden generar peligro (por ejemplo, tráfico aéreo, vial, instalaciones eléctricas, o nucleares, procesos industriales, etc.) debe ser considerada actividad peligrosa. Aun si bien es cierto que el software se lo destina a una actividad peligrosa per se, no es menos cierto que el medio empleado genera un riesgo adicional.

Como conclusión, corresponderá al interprete, en cada caso, conforme a las particularidades que ofrezca, considerar o no la inclusión de la actividad informática en la categoría de actividades peligrosas, a los fines del manejo del régimen probatorio. (Bergel, 1996)

3.- RESPONSABILIDAD CIVIL DE LAS EMPRESAS INFORMATICAS.

No ajenas al resto del mundo empresarial, la empresa informática se enfrenta, en general, a las mismas clases

de responsabilidad civil legal que cualquier otra empresa o entidad, por las reclamaciones formuladas por sus clientes, empleados, accionistas o terceros. No obstante, por las singularidades que la informática comporta, se han dibujado una serie responsabilidades nuevas, como lo es este campo desde el punto de vista del mundo del Derecho, que van más allá.

Las causas de las que puede derivar, tienen una naturaleza muy variada y diversa, así como también lo son los campos legislativos que la regulan. Por este motivo se indicarán las responsabilidades civiles más importantes que podrían afectar a una empresa de informática, siendo conscientes de que se hará de una forma muy genérica. (Lucas, 1999)

Partiendo de las premisas o conceptos anteriormente establecidos en torno a la responsabilidad civil, podríamos hablar de cuatro (04) fuentes básicas de las que puede nacer una Responsabilidad Civil legal, en el campo que nos ocupa:

1. Las derivadas del ilícito penal.

- Art. 116 del Código Penal Venezolano, que establece:
  "Son responsables civilmente los posaderos dueños de casas de ventas de víveres o licores, y cualesquiera otras personas o empresas, por los delitos que se cometieren en los establecimientos que dirijan, siempre que por su parte o la de sus dependientes haya habido infracción de los reglamentos de polícia".

- Art. 118 del Código Penal venezolano,que dice:
  "Son también responsables subsidiariamente los maestros y las personas dedicadas a cualquier género de industria por las faltas en que incurran sus discipulos, oficiales o aprendices en el desarrollo de su obligación o servicio".

2. Responsabilidad Extracontractual, por daños causados a terceros interviniendo culpa o negligencia. Art. 1190 y ss del Código Civil.

Art. 1190: " El padre, la madre, y a falta de éstos el tutor(...), los preceptores y artesanos son responsables del daño ocasionado por el hecho ilícito de sus alumnos y aprendices, mientras permanezcan bajo su vigilancia".

Por su parte, el Art. 1191 *ejusdem*, establece: "Los dueños y los principales o directores son responsables del daño causado por el hecho ilícito de sus sirvientes y dependientes, en el ejercicio de las funciones en que los han empleado", pongamos por caso el accidente de un visitante en las oficinas de la empresa que sufre una fractura por la inadecuada manipulación de algunos containers, por parte de sus empleados.

Dentro de este tronco, y comunes en su naturaleza, encontramos las siguientes otras clases:

-Responsabilidad Patronal frente a los empleados, por la falta u omisión de las medidas de Seguridad e Higiene en el trabajo.

El artículo 6 de la Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo de 1986. Parágrafo 2°, establece": Quien ocultare a los trabajadores el riesgo que corren con las condiciones y agentes mencionados (....), o trataren de minimizarlos, creando de este modo una falsa conciencia de seguridad o que de alguna manera induzca al trabajador hacia la inseguridad queda incurso en las responsabilidades penales respectivas con motivo de la intencionalidad y con la circunstancia agravante del fin de licro".

Esta disposición está en conjunción con el Artículo 560 de la Ley Orgánica del Trabajo de 1990, que consagra:

"Los patronos (...) estarán obligados a pagar a los trabajadores y aprendices ocupados por ellos, las indemnizaciones previstas en este Título por los accidentes y por las enfermedades profesionales, ya provengan del servicio

mismo con ocasión directa de él, exista o no culpa o negligencia por parte de la empresa o por parte de los tabajadores o aprendices".

-Responsabilidad de los Administradores, El texto de nuestro Código de Comercio, establece en el artículo 266:

"Los administradores son solidariamente responsables para con los accionistas y para con los terceros:

1° De la verdad de las entregas hechas en caja por los accionistas.
2° De la existencia real de los dividendos pagados
3° De la ejecución de las decisiones de la Asamblea
4° Y en general, del exacto cumplimiento de los deberes que les imponen la ley y los estatutos sociales".

Se trata esta de una responsabilidad solidaria de todos los administradores, de la cual únicamente se podrán librar aquellos que prueben, que no habiendo participado en la toma de decisión desconocían su existencia, o que conociéndola emplearon todos los medios para evitar el daño.

-Responsabilidad por Productos Defectuosos. Arranca esta legislación especial en nuestro ordenamiento, con la Ley de Protección al Consumidor y Usuario.

Tienen estas disposiciones en común, el deseo de establecer una protección jurídica especial hacia los consumidores y usuarios, frente a las consecuencias que las actuales economías de escala puedan llegar a producir. Se trata, no obstante, de textos diferentes, que establecen distintos niveles de protección, basados en diferentes técnicas jurídicas también. Pero para resumir, podríamos decir, que en común tienen, el qué dicha protección se establece en base a una objetivación de la culpa (facilidad probatoria del consumidor.), solidaridad entre los diferentes intervinientes en el proceso productivo (mayores posibilidades de hacer efectivo el cobro de las indemnizaciones) , y la creación de otros instrumentos de control y garantías para los consumidores, que se compensan en parte en el establecimiento de determinados límites cuantitativos.

La aplicabilidad de estas normativas en el campo que nos ocupa es claro cuando hablamos de distribución o venta a consumidores finales, ordenadores personales, software para dichos ordenadores, equipos de medicina, etc, pueden servir como ejemplos comunes. Más allá podríamos llegar si hablásemos simplemente de usuarios, tal como lo hace la Ley de Protección al Consumidos y al Usuario, e incluyésemos dentro de esta categoría, a cualquier empresa compradora de equipos o programas.

No obstante, dependiendo de cada regulación, como se decía anteriormente, se podrá hablar de diferentes clases de responsabilidades, según el grado de objetivación, la culpa exigida, o la parte en la puede recaer la carga de la prueba.

3. La derivada del cumplimiento de las obligaciones. Artículos 1.271 del Código Civil. Dice así el 1.271 de nuestro Código:

"El deudor será condenado al pago de los daños y perjuicios, tanto por inejecución de la obligación como por retardo en la ejecución (...)"

Se trata en suma de una responsabilidad civil surgida como consecuencia del cumplimiento defectuoso de un contrato, por los daños o consecuencias dañosas que una deficiente o mala ejecución del contrato pudiera acarrear a la otra parte del contrato.

Un ejemplo claro sería aquel que hace referencia a las posibles consecuencias derivadas de un desarrollo deficiente de un programa de software, por los daños causados a la persona que lo compra o utiliza.

Como todos conocemos no existe una regulación especifica referida a la informática, entre otras cosas porque la trascendencia de ésta nace mucho después de promulgado nuestro Código Civil, no obstante por analogía,

se puede estar ante tres tipos diferentes de contratos aplicables, la compraventa de bienes muebles, el contrato de arrendamiento de servicios, o el contrato de obra. En ocasiones nos encontramos ante figuras mixtas, es decir un contrato donde aparecen entremezclados los tres tipos de figuras antes descritas, por ejemplo en una operación en la que se venden o suministran diversos ordenadores, con el compromiso de desarrollar un determinado software, y además con un contrato de mantenimiento.

Dependiendo de la naturaleza de las diferentes obligaciones, el régimen que habrá que aplicar será diferente uno de otro, ya que las consecuencias también pueden ser muy diferentes. En efecto, muy distinta es una obligación de hacer o realizar un determinado trabajo en un periodo también determinado de tiempo, que un contrato de asesoramiento, en el cual la prestación consistirá en la pura realización del mismo sin un compromiso en el resultado.

4. Responsabilidad por incumplimiento de la norma Constitucional, a partir de la vigencia de la nueva Constitución de la República Bolivariana de Venezuela, se consagra en sus artículos 28 y 62 *respectivamente una regulación del tratamiento automatizado de datos de carácter personal.*

Se trata de una regulación Administrativa, en la misma no se introducen modificaciones en cuanto al ámbito penal o civil, por la cual se trata de proteger la privacidad de las personas, frente a los abusos que pudieran cometerse con el uso de los actuales sistemas informáticos. En especial se trata de proteger aquellos derechos constitucionales que hacen referencia, a la religión, la ideología, la salud, el origen racial, vida sexual, a quienes presta una especial tutela, si bien la misma se extiende en general al establecimiento de un sistema de control de datos, y garantías de control de los mismos para el ciudadano, sobre sus recursos económicos, sanciones, etc.

Además, se ha dejado a salvo la acción del perjudicado para acudir a la vía ordinaria, o la contencioso-administrativa, dependiendo de si los ficheros son de titularidad privada o pública.

Especial mención merecen las dispocisones, que en esta materia, nuestra Constitución de 1999. establece:

Titulo III: De los deberes, derechos humanos y garantías.

Capítulo I Disposiciones Generales

Art. 28: Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados de carácter público, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el Tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegitimamente sus derechos. De la misma manera podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas.

Capitulo III De los Derecho Individuales

Art. 62 Se garantiza el derecho al honor, a la intimidad, a la vida privada en cuanto aquellos que no trasciendan al interés público o social, y a la propia imagen, así como la privacidad y confidencialidad.

Se consagra, entonces el derecho de rectificación y destrucción; asimismo, se consagra el derecho a los datos personales y patrimoniales, pero se respeta la convención de Estrasburgo de 28 de enero de 1981, en lo concerniente a que: "los datos de carácter personal relativos a la salud o actividad sexual no son objeto de almacenamiento automatizado", pues sólo hace referencia a aquéllos datos de carácter público.

En resumen, y como decíamos al principio, la Responsabilidad Civil legal de las Empresas Informáticas, no difiere sustancialmente de la de cualquier otra empresa. No obstante, el mundo de la tecnología, la informática y las comunicaciones, abre nuevos espacios, y crea nuevas situaciones a las que el mundo del derecho tiene que ir dando respuesta puntual. El comercio electrónico y la seguridad del mismo, abren puertas a un nuevo mundo mercantil, que sin duda trastocarán las viejas instituciones del derecho, que tendrán que adaptarse al mismo.

4.- La Responsabilidad como institución jurídica en el marco de la Actividad Informática. La Responsabilidad en los Contratos Informáticos

El incumplimiento de toda ley, como se ha indicado, genera una responsabilidad, tanto desde la perspectiva de la pasividad frente a la norma como desde un comportamiento contrario a la misma.

Diferente de la responsabilidad por atentar contra la privacidad es la responsabilidad surgida por el incumplimiento de un contrato.

La responsabilidad contractual surge precisamente por incumplimiento de alguna de las cláusulas establecidas en el contrato. Ya hemos hecho referencia amplia al respecto cuando hemos hablado del contrato informático (*).

Esta denominación ha sido adoptada por la doctrina para designar a los contratos cuyo objeto está constituido por bienes y servicios informáticos, entendiendo por tales "todos aquellos elementos que forman el sistema -ordenador- en cuanto al hardware, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información", existiendo, por tanto, contratos sobre hardware, software y servicios informáticos distinguiéndose entre éstos, principalmente cuatro categorías: la compraventa, el suministro, el mantenimiento y el arrendamiento (de obra o de servicios) (García, 1998)

De acuerdo al contenido del contrato y a la naturaleza de los servicios prestados, podríamos decir que la relación contractual que une al servidor con cada una de las partes involucradas, es un contrato de arrendamiento o prestación de servicios informáticos, donde el servidor se obliga a ejecutar una determinada actividad. En los términos indicados en el art.1579 del C. Civil, "El contrato de obras es aquel mediante el cual una parte se compromete a ejecutar determinado trabajo por sí o bajo su dirección, mediante un precio que la otra se obliga a satisfacer". Esto significa que el servidor (arrendador) de cada una de las partes, en este caso, del titular, del proveedor de bienes y servicios, y del emisor (arrendatarios), se obliga a prestar un servicio (interconectar y suministrar la información en la red) a los diferentes usuarios a cambio de un precio cierto, configurándose una relación de tracto sucesivo que puede ser rescindida en cualquier momento por cualquiera de las partes.

La especialidad de los contratos informáticos radica en las obligaciones que asumen las partes, en este caso, además de las obligaciones propias del contrato de arrendamiento de servicios (la prestación del servicio y la remuneración), el servidor o el proveedor de acceso, deben cumplir las obligaciones de información sobre el funcionamiento del sistema para que el usuario pueda acceder a la información y manejarla correctamente y prevención sobre los riesgos y asesoramiento técnico, estando obligado el usuario por su parte a colaborar con el desarrollo del contrato cumpliendo con las instrucciones suministradas e informando al proveedor a tiempo sobre cualquier situación anómala. (Rico, 1999)

Precisamente, el tipo más numeroso de contratos informáticos, es el de bienes y servicios. Como ya se ha señalado, la responsabilidad vendrá determinada por el incumplimento de alguna de las obligaciones de las partes. En este sentido seguiremos a Isabel de Llamberterie (1993) al diferenciar la fase precontractual de la contractual a la hora de determinar las obligaciones susceptibles de incumplimiento.

En la fase precontractual las partes deberán observar diligencia debida y buena fe, sobre la base del principio de autonomía de la voluntad; en el caso de existencia de contratos de estudio y asesoría o de peritaje previo, la responsabilidad se exigirá de acuerdo al Código Civil.

(*) Ver Rodríguez, Gladys. (1999) "Principios Básicos de la Contratación Informática". En Revista de la Facultad de Ciencias Jurídicas y Políticas de la Universidad Central de Venezuela. No. 114. Caracas.

(*) Ver Rodríguez, Gladys. (1999). "Los Contratos Informáticos: Formación y Ejecución. En Revista Electrónica Internacional –Venezolana de Derecho e Informática (REIVDI).

Es así, que por ejemplo, en una operación de comercio electrónico, la relación que une al servidor con cada una de las partes se encuadra bajo la figura atípica de los denominados contratos informáticos, por lo tanto hablamos de una responsabilidad contractual.

En la fase contractual, y en lo que se refiere a contratos sobre bienes, habrá de considerar la vulneración de cualquier obligación contraída en relación con el hardware (instalación y mantenimiento completo por el suministrador) o con el software (especificación clara de las responsabilidades sobre el producto y legislación aplicable).

En lo referente a los contratos de servicios informáticos, habrá que tener en cuenta las características del tipo de servicio que se contrate, para delimitar las obligaciones contractuales (de desarrollo de software, de integración de sistemas, de suministro, etc.)

Otro aspecto, a considerar es quienes son las partes del contrato, y por tanto susceptibles de exigirseles responsabilidad, y atendiendo al ámbito jurídico contenido en la Ley de Protección al Consumidor y al Usuario, se consagra: "Se consideran **proveedores** las personas naturales o jurídicas de carácter público o privado que desarrollen actividades de producción, fabricación, importación, distribución, comercialización de bienes, prestación de servicios a consumidores o usuarios por los que cobren precios o tarifas".

En materia informática el proveedor es quien tiene la formación profesional con relación al objeto del contrato además, de los conocimientos en el área, debiendo contratar de buena fe e informar correctamente a la otra parte y proporcionar claridad a las cláusulas y obligaciones del contrato.

Por su parte la misma ley, dispone que: "Se consideran **usuarios** las personas naturales o jurídicas que como destinatarios finales, adquieran, usen o disfruten a título oneroso, bienes o servicios cualquiera sea la naturaleza pública o privada o colectiva de qienes los produzcan, expidan, faciliten, suministren, presten u ordenen".

En materia de informática el usuario, por contraposición al proveedor es el débil, pues carece de los conocimientos técnicos necesarios, lo cual conlleva a la creación de contratos de adhesión, dando paso a los abusos que generalmente se presentan en este tipo de contratos. Sin embargo, tiene el deber de informarse adecuadamente para cooperar con el proveedor, y capacitar apropiadamente a su personal para el manejo de los equipos a adquirir.

Una vez expuesto quienes participan en la contratación se hace necesario determinar si el hardware y el software pueden o no ser considerados productos elaborads o fabricados.

Con respecto al software, hay que diferenciar el software a medida, el software adaptado para el cliente y distribuido masivamente.

Los dos primeros no pueden – en principio – ser considerados como "producto elaborado", ya que prevalece aquí el criterio de creación técnica cietífica, vinculado a la prestación de servicios.

En cambio no cabe duda algna de que el software elaborado y distribuido en serie, cumple con todas las condiciones para ser considerado "producto elaborado".

En lo que respecta al hardware, se ha destacado que si bien es un producto, a diferencia de otros productos conserva algunas peculiaridades que pueden desempeñar un papel de gran importancia en el juicio de responsabilidad. Entre tales particularidades, están las siguientes:

a) Se trata de un producto que requiere una notable pericia en el uso. Esto nos debe conducir a considerar la posibilidad de culpa concurrente entre el fabricante y el usuario; ya que sea en el origen del daño, en el desarrollo de las operaciones accesorias, en la sustitución de piezas, en las alteraciones, etc.

b) Tratándose del hecho de que el hardware está estrechamente unido al software en el funcionamiento, puede darse en el daño producido un concurso entre el proveedor del hardware y del software, que de común están diferenciados. (Bergel, 1996).

Caso de Responsabilidad: El Proveedor de Software.

Básicamente la expresión "software" comprende tanto el algoritmo sobre la base del cual se elabora el programa, como el programa propiamente dicho, elaborado en lenguaje de máquina, y la documentación (manuales descriptivos y de funcionamiento) que sirven de soporte.

El algoritmo, expresado en lenguaje de alto nivel que no puede ser leido por la máquina se denomina "programa fuente" para diferenciarlo del programa traducido por el compilador en lenguaje de máquina, "programa objeto", que es el encargado de dar las concretas instrucciones a la máquina. (Rodríguez, 1998)

El modo y la fase en la cual el error puede ser introducido en el programa son múltiples, y en cada una de las hipótesis la inexactitud, aún mínima, puede ocasionar la quiebra de todo el sistema. En este sentido cabe señalar que el error puede aparecer en la elaboración del algoritmo, que por constituir la base esencial del programa lo traslada a toda su secuencia; puede surgir de la traducción del programa fuente en lenguaje de máquina o finalmente puede aparecer en la inrtroducción del programa objeto a la máquina, para su concreta operación.

Desde otro punto de vista, el programa puede ser concreto en su concepción, más elaborado en forma negligente (por ejemplo, carencia de un adecuado control o de duplicación de operaciones críticas); puede ser reabastecido por el usuario con datos de entrada inexactos, con inevitable error en la salida.

En atención a estas circunstancias la dificultad de caracterizar el daño derivado del software no sólo se debe al hecho de que la producción del daño es de difícil apreciación fáctica, casi imperceptible, sino también al hecho de que depende de razones de sistemática conceptual, en cuanto docrina y jurisprudencia no han definido aún de modo claro y uniforme la naturaleza jurídica del software. Esta problemática, de por sí compleja, crea dificultades tanto en la atribución de responsabilidad como en cuanto a la prueba del hecho generador del daño. Hay que tomar en consideración que el estudio actual de la técnica resulta difícil concebir un software sin errores.

Las soluciones en caso de daños derivados de un software, se tiene: que se deben diferenciar los casos de software a la medida, o standard, que es el distribuido en serie.

En los dos primeros casos la obligación del proveedor debe ser considerada obligación de resultado, que genera una responsabilidad objetiva, con la consiguiente incidencia probatoria. La prestación se satisface proveyendo al usuario de un programa que responda a sus requerimientos y sea adecuadao y eficiente. En el software standard, distribuido masivamente, el proveedor sólo responde por vicios redhibitorios que tornen inadecuado el programa para el uso previsto. Es una obligación de medios. Además, por ser un producto elaborado, se aplicarán los principios relativos a la responsabilidad del fabricante por vicios del producto.

Finalmente se hace evidente que en esta materia existe diferencia entre la responsabilidad contractual, que contrae el fabricante –proveedor ante el usuario; y la responsabilidad que contrae ante terceros por daños causados por defectos o vicios del sistema, de carácter extracontractual.

CONCLUSIONES.

La denominada tercera revolución producto de los avances tecnológicos en general y de la informática en particular, ha hecho imperante que el Derecho se plantee recuperar el control sobre las técnicas y aunque no se alcanzará un dominio absoluto, sin embargo, los esfuerzos se conforman por lograr un control estratégico.

Ha sido esta idea de desarrollo acelerado lo que ha provocado el surgimiento de una nueva sociedad, una "sociedad de riesgos tecnológicos"; así el régimen de responsabilidad presente desde las culturas remotas es quien primeramente incorpora la idea de riesgo.

La responsabilidad civil parte de un principio universal "nadie puede causar un daño injusto a otra persona, y en caso de causarlo, dicho daño debe ser reparado.

Ante este criterio universal aquel que participa en la actividad informática o telemática encuentra un grado de imputabilidad que lejos de ser arbitrario impregna de seguridad a los actos que en el contexto de los contratos informático, auténticos contratos de adhesión. Es así, que las mismas empresas informáticas, hoy, enfrentan las mismas clases de responsabilidad civil legal que cualquier otra empresa por las reclamaciones formuladas y que pueden significar una responsabilidad derivada del ilícito penal, por daños causados a terceros interviniendo culpa o negligencia, la derivada del cumplimiento de las obligaciones y la responsabilidad por incumplimiento de la norma constitucional.

Precisamente, ante el auge de la contratación de bienes y servicios informáticos, la responsabilidad vendrá también determinada por el incumplimiento de alguna de las obligaciones de las partes. En este sentido, sin embargo, es recomendable tener claro que en materia de responsabilidad en lo que concierne al software la producción del riesgo o daño es de difícil apreciación fáctica, además, se debe distinguir si se trata de un software a la medida o adaptado para el cliente y distribuido masivamente.

REFERENCIAS.

Bergel, Salvador. (1996) "Informática y Responsabilidad Civil". En D. Altmark y R. Bielsa. (Coordinadores). **Informática y Derecho. Aportes de Doctrina Internacional.** Vol. 2. Buenos Aires – Argentina.pp 152-229

Busnelli, F (1986). **Introducciión en Computers e responsabilitd civile.**

García, N. (1998) "La cuestión de la responsabilidad en el Derecho Informático". En **Revista Electrónica de Derecho Informático.** No. 2. Septiembre de 1998.

De Lamberterie, I. (1993). "Contratos Informáticos". En D. Altmark y R. Bielsa (Coordinadores) **Informática y Derecho. Aportes de Doctrina Internacional.** Vol. 4. Buenos Aires. pp7-32.

Lucas, J. (1999) "La responsabilidad civil de las empresas informáticas". **En Revista Electrónica de Derecho Informático.** No. 11. Junio de 1999.

Maduro, E. (1967) **Curso de Obligaciones. Derecho Civil III.** Caracas, Fondo Editorial Lius Sanojo. Colección Grandes Jurístas.

Nieto, A. (1994) **Derecho Administrativio Sancionador.** Madrid- España. 2da edición

Pardo, J. (1999) **Técnica, riesgo y Derecho. Tratamiento del riesgo tecnológico en el derecho ambiental.** Barcelona- España. Editorial Ariel, S.A.

Rico, M. (1999) "Responsabilidad Civil de los Intermediarios derivada del Pago con Tarjetas en el Comercio Electrónico a través de Internet". En **Revista Eelectrónica de Derecho Informático.** Número 17. Diciembre de 1999.

Rodríguez, G. (1998) "Protección Legal del Software". En **Revista Tachirense de Derecho.** Universidad Católica del Táchira No. 10. Enero-diciembre 1998. pp97-122.

Rodríguez, G. (1999) "Principios Básicos de la Contratación Informática". En **Revista de la Facultad de Ciencias Jurídicas y Políticas .** Universidad Central de Venezuela. Año. XLV. No. 114. Caracas. pp112-138.

Rodríguez, G. (1999) "Los Contratos Informáticos: Formación y Ejecución". **En Revista Electrónica Internacional- Venezolana de Derecho e Informática.** Mayo- Agosto 1999.

Savatier, R. (1947). **Cours de Droit Civil**. Deuxieme Edition. Librairie Generale de Droit et de Jurisprudence. Reu Soufflot 20. París.

Von Tuhr, A. (1934) **Tratado de las Obligaciones.** Traducido por W. Roces. Editorial Reus, S.A. Madrid- España.

Textos Legales:

Asamblea Nacional Constituyente. Constitución de la República Bolivariana de Venezuela. 1999.

Congreso de la República de Venezuela. Código Civil.

Congreso de la República de Venezuela. Código de Comercio.

Congreso de la República de Venezuela. Código Penal

Congreso de la República de Venezuela. Ley Orgánica del Trabajo

Congreso de la República de Venezuela. Ley Orgánica del Prevención, Condiciones y Medio Ambiente de Trabajo.

Congreso de la República de Venezuela. Ley de Protección al Consumidor y al Usuario.

"Respuesta del Derecho Positivo Peruano al Reto de la Fe Pública en Materia Informática"

Autor: José Ochoa Reyes (Perú)
- Abogado Egresado de la Pontificia Universidad Católica del Perú
- Con Estudios de Maestría en Derecho Empresarial en la Universidad de Lima
- Fedatario Juramentado con Especialización en Informática

Sumilla:

"La fe pública es institución jurídica sustantiva de nuestro derecho. En el ámbito privado se encuentra relacionada con la seguridad jurídica que se requiere para propiciar el dinámico y moderno crecimiento de las fuerzas económicas que se desenvuelven en el libre mercado, cumpliendo un rol fundamental al otorgar la certeza que requieren los agentes económicos en sus transacciones, propiciando el desarrollo del derecho en la normalidad al evitar que tengan que acudir y sobrecargar al oneroso Sistema Judicial. Pero, de ser el caso la fe pública debe crear en los Jueces la convicción de lo realmente ocurrido, contribuyendo de esta forma a facilitar y abaratar el proceso litigioso que estos conflictos implican.

La fe pública tradicional aplicada a los contratos donde las partes contratantes estan frente a frente, en presencia física, es superada por los que prescinden de ello. Hoy en día existen cada vez más transacciones en el libre mercado que se forman y perfeccionan por medios electrónicos, que se caracterizan porque no hay intervención personal entre las partes, ni existe el ámbito territorial, factores de horarios o tiempos, sino que la operación se perfecciona informáticamente y en tiempo real sin la intervención personal de las partes contratantes.

La fe pública tiene que responder a esta nueva realidad adecuando con eficiencia su certeza a las particulares características que presenta la informática."

1.- LA FE PUBLICA EN EL ORDENAMIENTO JURIDICO PERUANO

Mengual y Mengual clasifica a la fe en dos categorías: La fe sobrenatural o divina, y la fe natural o humana. La fe sobrenatural o divina, es aquella fe relativa a la creencia de las verdades reveladas de manera sobrenatural o por Dios. La fe humana es la creencia que prestamos al dicho o al hecho de otros hombres. Esta fe puede ser otorgada por hombres revestidos de autoridad por las leyes, y por hombres que no están revestidos de aquélla.

Cuando hombres que no están revestidos de autoridad para dar fe, testimonian algún acto u hecho, la fe será privada, porque no constituye prueba plena, sino, prueba testifical y documental privada. Pero, cuando hombres revestidos de autoridad por la Ley para dar fe la otorgan, ésta se convierte en pública y se constituirá en prueba plena de lo autenticado, facilitando de ésta manera la vida en normalidad de las personas y de sus distintas relaciones económicas y jurídicas.

Existen dos clases fundamentales de fe pública, la judicial y la extrajudicial o privada, que con algunas excepciones está reservada casi exclusivamente a los profesionales del derecho. Sin embargo, cabe resaltar que en determinadas circunstancias, se ha otorgado atribución fedante a determinados funcionarios en los casos en que por la frecuencia y especialización de las relaciones a proteger, aconsejan acudir a los servicios de otros fedatarios.[1]

La certeza en el campo privado se produce a través de la fe pública otorgada por determinados funcionarios públicos investidos de facultad fedante dentro del ámbito de su competencia. Deben facilitar con su fe, los medios convenientes para la prueba en caso que sobrevenga la anormalidad. Esta fe pública puede ser otorgada por los notarios o cualquier otro funcionario que, por disposición expresa de la Ley, tiene potestad y atribuciones como depositario de la fe pública en un ámbito de competencia, teniendo como denominación genérica la de "Fedatarios".

[1] Gutierrez del Solar, Eduardo, Ob.Cit. pg.4.

La legislación peruana, con fuertes raíces latinas, tiene como institución principal de la fe pública en las relaciones privadas al Notario, por ello, el sistema es denominado como del *"Notariado Latino"*. El Artículo 2º del Decreto Ley Nº 26002, Ley del Notariado, define al Notario y le atribuye funciones de la siguiente manera:

"El Notario es el profesional del Derecho que está autorizado para dar fe de los actos y contratos que ante él se celebran. Para ello formaliza la voluntad de los otorgantes, redactando los instrumentos a los que confiere autenticidad, conserva los originales y expide los traslados correspondientes.

Su función también comprende la comprobación de hechos y la tramitación de asuntos no contenciosos previstos en la Ley de la materia".

Esta definición y funciones coinciden en esencia con las establecidas en el primer principio fundamental del Notariado Latino del Primer Congreso Internacional del Notariado Latino (U.I.N.L.), celebrado en Octubre de 1984, y de la cual el Perú es país fundador, donde se define al Notario como:

> *"...el Profesional del Derecho encargado de una función pública consistente en recibir, interpretar y dar forma legal a la voluntad de las partes, redactando los instrumentos adecuados a ese fin y confiriéndoles autenticidad. Conservar los originales de éstos y expedir copias que den fe de su contenido. En su función está comprendida la autenticidad de hechos".*[2]

El Perú mantiene un Notariado independiente, conceptualizando al Notario como el "profesional del derecho que accede al cargo por concurso público y es investido de la función fedante mediante un título expedido por el Estado, garantizando de esta manera la independencia e imparcialidad de sus actos".

La función notarial tiene un contenido complejo, pues no solo da fe pública, sino que, además, certifica hechos y asesora a las partes del negocio jurídico de una manera imparcial, promoviendo el conocimiento del derecho. Ejerce su función fedante en forma personal, autónoma, exclusiva e imparcial, de manera privada. Sus funciones, están referidas a la autorización que tiene para dar fe de los actos y contratos que ante él se celebran, formalizando la voluntad de los otorgantes, redactando los instrumentos públicos por mandato de la Ley o a solicitud de las partes, a los que confiere autenticidad, conservando los originales y realizando los traslados correspondientes.

Pero el sistema jurídico peruano tambien permite la existencia de otros funcionarios con capacidad fedante en determinados ámbitos de competencia, previa autorización por Ley. Existen diversas leyes que otorgan a entidades del Estado, en el ámbito de sus relaciones de derecho privado, la facultad de contar con Fedatarios - *No Notariales* -, que autentican y confieren fe pública a los documentos extendidos por esas instituciones.

Estos Fedatarios, tienen otra forma de actuación *"Fedante"*, más inspirados en el sistema anglosajón, cuya orientación legal da preferencia al testimonio verbal o credibilidad de lo actuado por las personas, sustituyendo en gran parte al documento notarial. El sistema permite trasladar la función de depositarios de la fe pública a personas que no necesariamente tienen que ser profesionales del derecho, pero con funciones mucho más limitadas que las notariales.

En sentido estricto, en el sistema anglo - sajón la función del Notario o *"Notary Public"* se limita básicamente a la certificación de firmas y pueden constituirse en tales, cualquier persona que reúna condiciones mínimas de credibilidad.

En el caso peruano, estos funcionarios no notariales con facultades *"Fedantes"* tienen un ámbito de competencia más amplio que el notario anglo-sajón, ya que no sólo certifican firmas, sino, además, las resoluciones y documentos que sus instituciones extienden, e inclusive de "hechos", tal como sucede en el caso de los Fedatarios de la Superintendencia Nacional de Administración Tributaria - SUNAT-.

En función a esta delegación de facultades, es que los ministerios, municipalidades, funcionarios consulares, jueces de paz letrados y no letrados, diversos organismos de derecho público, universidades, tanto estatales como

---

[2] Revista del Colegio de Notarios de Lima, "Article_Title," Notarius Año 1, Nº 1 (1990): pp. 22 y 47-49.

privadas, párrocos etc., tienen fedatarios que autentican todas las resoluciones y documentos que ellos extienden, así como en determinados casos, *" de hechos acaecidos bajo su competencia"*.

Pero en todos los casos, incluidos los notarios, cabe recalcar que los agentes privados con facultades fedantes no tienen la potestad de declarar su derecho a dar fe en forma coercitiva, ni a restablecer la normalidad de la legalidad en el ámbito de su competencia. Su fe pública tiene esencialmente un fin preventivo, buscando desanimar el incumplimiento por cualquiera de las partes intervinientes en un contrato, facilitando o generando los medios convenientes para que la prueba surta efectos de certeza en caso que sobrevenga un conflicto de intereses.

Siendo la fe pública regulada por normas con rango de Ley, en el Perú no existe un sistema unívoco de actuación fedante, sino que se ha establecido un sistema mixto aplicable a las relaciones jurídicas de derecho privado, donde el Notario representa al sistema latino, y los demás Fedatarios, representan de alguna forma, la practicidad del sistema anglosajón.

2.- LA INFORMATICA Y LA FE PUBLICA TRADICIONAL FRENTE A LA CONTRATACION ELECTRONICA E INTERNET.

2.1.- La Fe Pública y la Contratacion Electrónica.

La Informática se encuentra cada vez más ligada con el Derecho y por ello, en *"las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades de las modernas tecnologías de la información, surgen los problemas de cómo resolver determinados conflictos nacidos de éstas relación"*.[3]

La **"Informática"**, acrónimo de "información automática o automatizada", es la ciencia de la información y se refiere a todo lo que tiene relación con el procesamiento, transmisión y almacenamiento de datos e información utilizando computadoras.

Tal como menciona el Dr. Julio Nuñez Ponce en su obra, "Derecho Informático, Nueva Disciplina Jurídica para una Sociedad Moderna": Los problemas de carácter metodológico y operativo que la Informática plantea al jurista contemporáneo pueden definirse como *"... los problemas de una frontera nueva del derecho, que abre una perspectiva que aún ha de trazarse, ya que el nuevo territorio se extiende al futuro, ... la Sociedad tecnológica, cuya protagonista es la computadora, está caracterizada por la rapidez de su desarrollo y de sus innovaciones que obligan al observador a proceder en el sentido mismo de una experiencia en formación"*. [4]

La informática a pasado ha tener un un rol esencial en todas las ramas del quehacer humano. No se trata que tenga cada vez más influencia o importancia, sino, que con ella, o, a través de ella, giran y se sustentan la mayoría de las actividades humanas, sean de aprendizaje, investigación, comunicación, relaciones sociales, relaciones jurídicas y económicas.

Tal como ha sido conceptuada y plasmada la fe pública tradicional en nuestro ordenamiento jurídico, deviene en insuficiente cuando se trata de materia infomática, en especial, tratándose de la denominada contratación electrónica, que prescinde de la presencia física de las personas, de horarios y espacios determinados.

Miguel Angel Dávara define la contratación electrónica como aquella: "Que se realiza mediante la utilización de algún elemento electrónico **cuando éste tiene, o puede tener, una incidencia real o directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo**".[5]

3 Davara Rodriguez, Miguel Angel: "Derecho Informático", Editorial Arazandi S.A., Navarra, 1993, pg.26.

4 Nuñez Ponce, Julio, "Derecho Informático: Nueva Disciplina Jurídica para una Sociedad Moderna." Lima, Perú, 1996. ed., s.v. pág.3, De Informática y Derecho, Frossini, Vittorio.

5 Dávara, Miguel Angel, Derecho Informático (Pamplona, España: Ed. Aranzandi, 1993) pp. 183.

A su vez, Carlos E. Saltor se refiere a los Contratos Telemáticos como aquellos que se caracterizan, no por el objeto sobre el que recaen, **"sino por la forma de perfeccionamiento por medio de un sistema telemático"**.[6]

Hoy en día, se celebran transacciones comerciales con trascendencia jurídica viajando en avión, en tren, de vacaciones en un páramo lejano o encontrándose las partes inclusive en distintos países y en cualquier horario. Se efectúan millones de transacciones vía tarjetas electrónicas (donde la otra parte viene a ser una computadora), que son una modalidad de contratación electrónica.

Pero la contratación electrónica posee otra característica que trastoca al derecho tradicional. Cada vez más de éstas operaciones comerciales se realizan sin el uso del documento escrito, se perfeccionan a través de documentos en soporte y lenguaje digital, que es el lenguaje de las computadoras. La utilización del documento digital aumenta drásticamente - día a día - y es cada vez de mayor trascendencia en las transacciones comerciales informáticas y, ésta, es una realidad que el Derecho no puede desconocer.

Regresando a la institución de la fe pública tradicional, si nos ceñimos estrictamente a lo establecido en el Artículo 2º de la Ley del Notariado, *"El Notario es el profesional del Derecho que está autorizado para dar fe de los actos y contratos que ante él se celebran. Para ello formaliza la voluntad de los otorgantes, redactando los instrumentos a los que confiere autenticidad, conserva los originales y expide los traslados correspondientes"*.

El Notario tiene facultades de dar fe pública, pero sólo en aquellos casos en que intervenga personalmente, no existiendo la posibilidad de desligar tal circunstancia de su función fedante. Pero, el tener que acudir a un determinado lugar o ante una determinada persona en un horario pre establecido para perfeccionar una operación por medios electrónicos al cual se le requiera dotar de certeza, le resta todo sentido a los beneficios de costos, tiempos y costos que la informática conlleva.

Los nuevos retos planteados a la fé pública en materia de contratación electrónica exigen del Derecho la creación de instituciones que sepan incorporar junto con poderosas y modernas tecnologías, recursos humanos altamente especializados y estructuras empresariales altamente eficientes, con suficientes recursos de capital para hacer frente óptimamente a las nuevas formas de contratación electrónica, que necesitan de seguridad jurídica ***"informatizada"*** y no ***"personalizada"***, y a los demás desafíos y exigencias que el actual entorno mundial informatizado - *ya altamente masificado* -, y el futuro que tal sector, requieren.

Hoy en día, solo en contados casos será indispensable la reunión personal entre los intervinientes y el Notario, porque tanto para los primeros, como para el mismo Notario, el tiempo es valioso y la información debe ser procesada y vuelta a enviar a su destino, al menor costo y con la mayor rapidez, seguridad y de la manera más óptima posible.

A medida en que los entornos informáticos se vuelven cada vez más sofisticados, los riesgos son más complejos o de circunstancias nuevas, por lo que sus operadores, han de tener una preparación más profunda, tanto teorica como procedente de la experiencia.[7]

En el actual contexto, para ser eficientes y competitivos, se hace cada necesaria la concentración de conocimientos, recursos económicos, tecnológicos y la conjunción de personal altamente especializado.

La problemática de la fe pública en materia informática, así como muchas otras derivadas de su utilización masiva en todas las esferas de las relaciones humanas con trascendencia jurídica, corresponde resolverlas mediante la conjunción óptima de las instituciones propias del Derecho Notarial con las del Derecho Informático.

---

6 Saltor, Carlos E., "Informática y Contratos". diss., (Bariloche, Argentina: Ponencia presentada en el IV Congreso Iberoamericano de Informática y Derecho., 1994).

7 Del Peso Navarro, Emilio - Ramos Gonzales, Migue Angel: "Confidencialidad y Seguridad de la Información", Edit. Díaz Santos S.A., Madrid, 1994, pg.52.

2.2.- La Fe Pública e Internet.

Para muchos, la mayor utilidad que ha significado la Informática se a producido cuando ésta se ha unido con las Telecomunicaciones, creando la llamada "Teleinformática o Telemática", donde la información viaja a la velocidad de la luz en redes ópticas, cable u otras tecnologías equivalentes y que se ha traducido en una nueva visión del mundo y de lo que va a significar el progreso en el crecimiento de las personas y de las sociedades en general.

La Telemática a impulsado el desarrollo de nuevas y sofisticadas tecnologías, las que son utilizadas por los agentes económicos de inmediato, sin más preámbulos que su puesta a disposición en el mercado. Pero, con su uso masivo, en el ámbito económico se ha producido el nacimiento de problemas jurídicos no previstos, que requieren para su entendimiento y solución de un alto grado de conocimientos y especialización.

Nuevas instituciones como Internet, el Correo Electrónico, el Módem, las Computadoras en redes y muchas otras, están siendo objeto de estudio y regulación, porque junto con ellas está naciendo su contrapartida, es decir, nuevas formas de conflictos sociales y el aprovechamiento indebido que determinadas personas buscan obtener de sus ventajas, naciendo por lo tanto, también nuevos delitos.

Quizás, la de mayor trascendencia sea INTERNET, que como red pública de comunicaciones se encuentra incluída en la legislación de telecomunicaciones peruana como un servicio de valor añadido y como tal, las empresas que presten servicios de Transferencia Electrónica de Datos Informatizados - E.D.I. -, transferencia electrónica de fondos, comercio electrónico y otros servicios considerados por la ley como de valor añadido, deben cumplir con una serie de obligaciones, tales como inscribirse en registros especiales y encontrarse bajo la supervisión de OSIPTEL con respecto a la calidad, libre y leal competencia, facturación y continuidad en la prestación de los servicios.

Pero, el problema se les presenta a los agentes económicos, es el conocer con certeza la fiabilidad de la información que circula por la Red. El tema de la Información que circula por la Red cobra relevancia cuando se ven involucrados intereses con relevancia económica o jurídica de empresas o gobiernos.

Como menciona el Dr. Julio Nuñez Ponce[8], *"el uso indebido de la red, puede originar problemas jurídicos que es necesario preveer para solucionarlos adecuadamente... Dentro de los problemas jurídicos en Internet tenemos los siguientes:*

> *Libertad irrestricta de los menores de edad para acceder a la información indecente o pornográfica, infracciones del derecho de autor de las creaciones intelectuales incluidas en las páginas web, vulneración del derecho a la intimidad, daños producidos por virús informáticos, valor probatorio de los documentos informáticos contenidos en Internet, estafas electrónicas, libertad de información basada en información inexacta, entre otros".*[9]

Todos estos problemas con trascendencia jurídica, devienen en nuevas áreas de solución para el Derecho y, donde la fe pública debe ingresar para otorgar una certeza de la que carece hoy en día.

El problema se agrava, por cuanto el principal peligro de la red radica justamente en su principal beneficio, el de la rapidez con la que viaja la información, tan sólo en cuestión de segundos de que alguna información falsa sea soltada en algún lugar del planeta, el resto puede enterarse antes de producirse cualquier reacción que pudiese resultar en una protección efectiva. Es por ello, que el mundo se ha dado cuenta de lo vulnerable y peligrosa en que se puede transformar Internet a la hora de difundir información inexistente o falsa.

---

8 Nuñez Ponce, Julio, Ob. Cit. anterior.

9 Subrayado agregado.

Esta realidad ha hecho que la **NASDAQ**, la bolsa electrónica de E.U.A., se haya visto obligada a desarrollar un "instrumento de vigilancia" (surveillance device), para permitir detectar información falsa en Internet que pueda haber sido lanzada con la intención de afectar un valor determinado.

La National Association of Security Dealers (NASD) ha lanzado también un programa para instruir a los agentes de valores sobre la conveniencia o no de usar Internet como instrumento de obtención de información sobre los mercados. Tampoco se descarta la posibilidad de que aparezca la figura del **"Red Notario"** que ***"certifique"*** la fiabilidad de una información en la Red.[10]

3.- LA FE PUBLICA Y EL DERECHO INFORMATICO.

Como se ha mencionado, el término "Fe" proviene del latín "*facere*" y consiste en el crédito que se dá a una cosa por el hecho de que quien la otorga es un funcionario premunido de autoridad.

Pero, la Informática se encuentra cada vez más ligada con el Derecho y por ello, en *"las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades de las modernas tecnologías de la información, surgen los problemas de cómo resolver determinados conflictos nacidos de éstas relación"*.[11]

En materia informática, necesariamente hay que hacer referencia a "procesos", sean estos informáticos, electrónicos o de otras tecnologías equivalentes, por lo que se ha requerido de una adaptación y reestructuración de los principios rectores que regulan la fe pública desde la perspectiva tradicional hacia su integración al interior de estos procesos tecnológicos.

Para que la fe pública produzca certeza en materia informática, es necesaria su integración eficiente con las tecnologías de información a través de nuevas instituciones surgidas del "Derecho Informático". El Derecho Informático es la rama especializada del Derecho que tiene por objeto de estudio a la informática y los nuevos problemas jurídicos que le plantea al Derecho su uso masivo y cada vez más trascendente en todo tipo de relaciones humanas.

El procesamiento, transmisión y almacenamiento de la información y el uso que de ella se esta realizando masivamente - *no sólo cuantitativa, sino también cualitativamente* -, a través de la informática y las telecomunicaciones, enfrenta al Derecho Informático con el acuciante problema de encontrar soluciones prácticas y modernas para el otorgamiento de una adecuada fe pública para otorgar certeza a estas operaciones informatizadas con relevancia jurídica, sin que por ello, se atente contra la inmediatez y dinámica propias de estas operaciones.

Desde el punto de vista jurídico - informático, consideramos que son tres los principales retos que la informática le plantea al Derecho Informático con relación a la fe pública, para que éste haciendo uso de instituciones propias los resuelva con creatividad e innovación:

"a) La de otorgar certeza a la contratación electrónica y en la transmisón de información por medios telemáticos.

b) La de otorgar certeza a los procesos informáticos, dirigiendo y responsabilizándose de la adecuada utilización de las herramientas que le proporciona la informática jurídica para convertir los archivos tradicionales "pasivos" en archivos digitales " interactivos".

c) La de servir de agente promotor en la reducción de costos operativos y administrativos al interior de las organizaciones económicas y propulsor de la eficiencia y competitividad empresarial."

---

[10] Arturo Catalán, "Lo Falso en la World Wide Web", de "El Mercurio", Santiago de Chile - Grupo de Diarios de América - (acatalan@mercurio.cl).

[11] Davara Rodriguez, Miguel Angel: "Derecho Informático", Editorial Arazandi S.A., Navarra, 1993, pg.26.

El Derecho Informático debe convertirse en un instrumento idóneo para propiciar la eficiencia y competitividad de los agentes económicos en el nuevo contexto mundial, proponiendo soluciones creativas e innovadoras para enfrentar válidamente las nuevas problemáticas planteadas a la fe pública para otorgar certeza a las operaciones económicas privadas realizadas informáticamente.

4.- LA RESPUESTA DEL DERECHO POSITIVO PERUANO AL RETO DE LA FE PUBLICA EN MATERIA INFORMATICA

El Derecho Positivo Peruano ha respondido al reto de la fe pública en materia informática a través de la dación de una serie de normas legales donde interactuan instituciones propias del derecho notarial e informático y de las tecnologías de la información y comunicaciones en forma tal, que permiten la creación de un depositario de la fe pública en materia informática que pueda otorgar certeza jurídica y tecnológica a documentos electrónicos convertidos en imágenes inalterables e individualizables denominadas microformas digitales.

A partir de un conjunto de instituciones básicas propias de nuestro derecho y una aplicación consistente de las tecnologías, entre las cuales podemos mencionar a la novísima fe pública informática, los procesos tecnológicos idóneos y el documento resultante, la microforma digital, las normas legales peruanas estructuran un sistema denominado *Sistema de Microformas Digitales*, que se integra coherente y eficientemente dentro de nuestro ordenamiento jurídico nacional y se halla armonizado con los más altos estándares jurídicos y técnicos internacionales sobre la materia.

El Decreto Legislativo 681 y su Reglamento - D.S. Nº 009-92-JUS, la Ley 26612 y su Reglamento - D.S. 002-98-ITINCI, el Decreto Legislativo 827 y demás normas complementarias, modificatorias y reglamentarias sobre promoción a la inversión privada y modernización de la gestión pública y privada en el Perú, crean el Sistema de las Microformas Digitales con el que se consigue otorgarle al documento informático características de inalterabilidad, confiabilidad, autenticidad e individualidad suficientes como para crear la convicción de prueba plena durante todas las fases tecnológicas de la vida de un documento electrónico, es decir, el de su confección, almacenamiento, transmisión y recuperación, de modo tal que cuente permanentemente con la certeza necesaria para convertirlo en objeto de protección jurídica.

Existen diversas áreas y materias informáticas y telemáticas que han sido objeto de un reconocimiento jurídico formal en nuestra legislación vigente, entre otros, en la seguridad jurídica de los archivos digitales - (*Art. 8º Dec. Leg 681)*; en los procesos de captura automática de datos - (*Art.5º Dec. Leg. 681)*; en la Signatura Electrónica - (*Art.3º Ley 26612)*; en la Conversión de los Archivos tradicionales de las entidades bancarias y financieras por Archivos de Microformas - (*Art. 6º Ley 26612)*; en el Intercambio Electrónico de Datos (EDI), en el Comercio Electrónico y en otros Servicios de Valor Añadido - (*Art. 9º Ley 26612).*

El Sistema de Microformas Digitales resulta en un novedoso sistema jurídico – tecnológico que integra la institución de la fe pública surgida del Derecho Notarial e Informático, con las tecnologías informáticas y de comunicaciones (TIC) de elaboración, administración y gestión de imágenes, convergentes hacia la problemática específica del valor probatorio y efectos legales plenos de documentos informáticos que han sido convertidos a imágenes digitales inalterables e individualizables (microformas digitales), a través de procesos de micrograbación, la intervención de depositarios de la fe pública en los procesos informáticos y la introducción de medidas de seguridad jurídico – tecnológicas auditables y verificables.

Dentro de los nuevos conceptos e instituciones creadas por el régimen legal del Sistema de Microformas, destacan la de tres instituciones fundamentales, el de la ***"Microforma digital"***; el ***"Proceso Tecnológico Idóneo"***; y el ***"Depositario de la Fe Pública Informática"***.

Se otorga **"certeza jurídico - tecnológica"** a las imágenes convertidas en **"microformas digitales"** utilizadas en materia de archivo de documentación e información elaboradas por medios informáticos y telemáticos almace-

---

12 Instituto Nacional de Defensa de la Competencia y la Propiedad Intelectual.

nadas en **"microarchivos"**, que se han confeccionado mediante procesos tecnológicos idóneos de micrograbación, cumpliendo con los **"requisitos técnicos"** - *Normas Técnicas aprobadas por el INDECOPI*[12] - y **"requisitos formales"** - *Bajo la dirección y responsabilidad de uno de los depositarios de la fe pública conforme al Decreto Legislativo 681* -, lo que permite su posterior transmisión telemática segura.

El sistema de microformas digitales incorpora las seguridades tecnológicas que cumplan con las estándares técnicos mínimos internacionalmente aceptados sobre la materia, o de cualquier tecnología que los supere.

Entre las seguridades tecnológicas aceptadas se encuentra el de la signatura electrónica. Se puede identificar si la signatura electrónica en un documento digital ha sido alterada o modificada, dependiendo del grado de seguridad adoptado. Existen medidas de seguridad como las llaves de terminal, códigos, claves de identificación así como recurriendo a ciertas características físicas como la huella digital, reproducción de la voz, geometría de la mano, huellas de los labios, passwords, etc. Igualmente, los sellos del software sirve para detectar si hubo o no alteraciones rechazando cualquier cambio.

Las soluciones jurídicas que se adopten van a depender de las seguridades técnicas que posean los sistemas de almacenamiento y transmisión para evitar la alteración de los mensaje, lograr la identificación del expedidor o destinatario del mensaje transmitido, y la verificación formal del mensaje y la autenticidad del mismo.

Se exige que las microformas se confeccionen cumpliendo con el Proceso tecnológico idóneo, donde se incluyen los requisitos técnicos, pero además, deben cumplir con los requisitos formales establecidos en el Decreto Legislativo 681º, normas complementarias y reglamentarias, para efectos de que puedan sustituir al documento original para todos los efectos legales.

Si el Proceso de Micrograbación de Microformas ha sido efectuado bajo la dirección y responsabilidad de un depositario de la fe pública informática, dando fe pública de que se han cumplido con todos los requisitos formales y técnicos establecidos, las microformas adquieren por sí, un valor probatorio pleno, pudiendo sustituir a los documentos originales para todos sus efectos, por lo que si estos se encuentran en soporte papel pueden ser destruidos por sus titulares si así lo decidieran[13].

El depositario de la fe pública cumple el rol del tercero certificador neutral, como dador de una nueva clase de fe pública - la fe pública informática -, que a diferencia de la fe pública tradicional, no se otorga en base a la autentificación de la capacidad de personas, del cumplimiento de formalidades en los instrumentos notariales o a la certificación de hechos, sino, que se aplica a la certificación de procesos tecnológicos, de resultados digitales y códigos y signaturas electrónicas.

Se constituye en una nueva institución surgida del Derecho Informático y se espera entre otros que otorgue seguridad jurídica a los procesos informáticos, dirigiendo y responsabilizándose de la adecuada utilización de las herramientas que le proporciona la informática jurídica, para confeccionar documentos informáticos con certeza plena y convertir los archivos tradicionales en archivos digitales; servir de agente promotor en la reducción de costos operativos y administrativos al interior de las organizaciones económicas y propulsor de la eficiencia y competitividad empresarial y otorgar certeza en la contratación electrónica y la información convertida en microformas digitales.

CONCLUSIONES.

Sobre la base de tres instituciones jurídico – tecnológico básicas, la fe pública informática, los procesos tecnológicos idóneos y la microforma digital, la legislación peruana construye un sistema que proporciona el sustento de la certeza en la seguridad jurídica y tecnológica que otorga la fe pública informática inmersa en el Sistema de Microformas, encontrándose entre sus principales características el que sea auditable por medios técnicos idóneos,

13 Artículos 7º, 8º y 16º del Decreto Legislativo Nº 681 del 14/10/91.

de simple entendimiento, incluso por personas no expertas en tecnologías y en el de su sustentación ante autoridades judiciales, de supervigilancia o extrajudiciales en forma de secuencia jurídico – lógica.

El Derecho tiene que avanzar de la mano con la realidad informática, sin entorpecer su desarrollo y crecimiento y desde ésta perspectiva, el Sistema de Microformas Digitales propuesto por el Derecho Positivo Peruano plantea una interesante alternativa jurídico - tecnológica para solucionar la incertidumbre que aún mantiene a los agentes económicos recelosos de la utilización masiva del documento informático en sus operaciones económicas, permitiendo así establecer las bases para una fe pública en materia informática.

Obligaciones Pactadas Mediante Medios Informáticos

Aída Noblia (Uruguay)
Escribana

I – INTRODUCCION

Los medios informáticos constituyen uno de los posibles soportes de las diversas formas en que se expresa la voluntad o se realiza la declaración que contiene el pacto obligacional o la manifestación de esa voluntad que exterioriza la esencia del negocio jurídico.

La existencia de tales medios no hace confundir de ninguna manera la tarea del operador jurídico con la del operador informático, como no se confunden con la de éste las del médico, arquitecto, ingeniero, etc., sino que torna a la informática como técnica complementaria de toda profesión, incluso de toda actividad humana económica e intelectual debido a su potencialidad.

Sin embargo, desde el punto de vista del Derecho, en especial de las obligaciones, los nuevos medios informáticos, alteran el soporte material en el cual se expresa actualmente la voluntad, a veces en parte, a veces en su totalidad, y al hacerlo, provoca la necesidad de crear nuevos mecanismos que cumplan las mismas finalidades para las cuales fue creado el soporte papel, que se adecuen a estos nuevos medios.

II – FINALIDADES Y MODIFICACIONES EN LOS MEDIOS – BREVE HISTORIA

El hecho reitera situaciones ya planteadas en la historia de las obligaciones y los pactos; si bien el Derecho Romano arcaico era esencialmente formalista, como todos los derechos primitivos, "la producción de los efectos jurídicos predeterminados, venía ligada, única y exclusivamente, al cumplimiento de prácticas o ritos predeterminados, indispensables para que surgieran tales efectos, y suficientes para originarlos..." según expresa Antonio Rodríguez Adrados (*), diferenciándose el derecho romano de otros derechos de la antigüedad, por la amplia utilización d elos "verba", determinadas palabras, cuya pronunciación en aquellos ritos era esencial, construyéndose en el caso de la "stipulatio" la estructura toda del negocio, sobre la oralidad.

Los soportes materiales han cambiado a lo largo de la historia; las tablillas de madera utilizadas durante la vigencia del derecho romano clásico, fueron sustituidas por el pergamino de tela, luego de cuero, los documentos no se firmaban en la Roma antigua, sino que otorgantes y testigos y aún el "Tabelio", colocaban un sello en señal de asentimiento, y ese sello muchas veces era el mismo utilizado por el otorgante, los testigos y el tabelio; cuando comenzaron a "firmarse", tal firma no era como hoy, la reproducción del nombre, sino una frase escrita al final del texto, con relación al contenido del documento.

Pero la diversidad de los medios a través de los cuales se constituía la obligación, tenía en esos tiempos la misma finalidad que tiene el documento escrito y firmado tal como lo conocemos hoy, en los albores del tercer milenio: conferir certeza a la negociación y al tráfico jurídico de bienes, probar su existencia, solemnizar el acto que daba origen a las obligaciones.

La cantidad de testigos que se utilizaban, (cinco, en principio, que representaban las cinco clases en que se dividía la sociedad) además de determinados rituales y palabras que necesariamente debían pronunciarse durante el acto solemne, constituían a la vez la forma en que podrían probarse las obligaciones contraídas y la misma existencia del "vinculus iuris", si así fuere necesario.

La relación obligatoria nacía para los romanos clásicos del cumplimiento de tales solemnidades, no siendo trascendente al derecho la interpretación de la voluntad sino que cumplidos los ritos se daba por sentado el consentimiento de las partes. La palabra "contractus" derivada etimológicamente del verbo "contrahere", originaria-

mente no tenía un significado técnico jurídico preciso; cuando comenzó a utilizarse, se le dio el sentido de "lo contraído", lo derivado del pacto, este sí, acuerdo de voluntades entre las partes; pero el Derecho romano, como explica Messineo, no identificaba el contrato con el acuerdo o acto de voluntad común de ambas partes; lo que da nacimiento a la relación obligatoria es el cumplimiento de las solemnidades; la concepción que identifica al contrato con la declaración de voluntad común, que se plasmó en los Códigos occidentales del siglo XIX tiene su origen en el concepto de autonomía de la voluntad o autonomía privada que se desarrolló a partir de las concepciones individualistas que dieron origen a la Revolución Francesa.

En cuanto a la forma oral o escrita, la norma general para los contratos entre vivos, dictada por Justiniano en el año 528, fijaba la regla de que todos los contratos podían, en principio hacerse en forma oral o por escrito, marcando el "indeferentismo dualista" entre oralidad y escritura, que permaneció vigente en España hasta el Código Civil, sin ser afectada por Las Partidas de Alfonso el Sabio ni por la Pragmática de Alcalá, en este sentido, aún cuando se introdujeran modificaciones incluso en esta última, en que se busca eliminar del documento toda oralidad que no fuera la lectura del mismo, concretamente de la ntoa o carta, que del mismo tomaba el Notario en el "Libro de protocolo". El documento sólo constituía un medio de prueba de las obligaciones pero no era esencia de las mismas.

En el derecho germánico antiguo, la trasmisión del dominio se realizaba en dos etapas, no dándose plenamente como en el derecho romano clásico la unidad de acto y la inmediación; primero se efectuaba la "auflassung", declaración del trasmitente manifestando el desprendimiento del bien y la aceptación del precio y luego, se producía la "gewere", acto físico de toma de posesión del bien por el adquirente; la "auflassung" fue sustituída posteriormente por la "chartae", documento unilateral redactado por el Notario, conteniendo la voluntad del trasmitente, y la "guewere" fue sustituída por la "levare chartae", acto por el que el adquirente tomaba el documento como exteriorización de su voluntad de adquirir el bien.

Durante la Edad Media la inalterabilidad de la nota (skeda) que tomaba el Notario y conservaba en su poder quedaba confiada a éste, al igual que la redacción de la carta que a pedido de las partes extendía a veces luego de mucho tiempo, in extenso, en caso de que existieran discrepancias y por tal motivo se la requirieran.

En la Época Moderna el principio de la autonomía privada introduce normas interpretativas que obligan a investigar el consentimiento de las partes, mientras en la forma la oralidad persiste, aún en el "acto del Notario", en la propia lectura, consentimiento y firma en un acto unitario, al que los glosadores denominaron "audientia"(de oír), "puesto que las declaraciones de las partes se hacen normalmente de palabra", según Rodríguez Adrados, denominándose "auscultatio"(de escuchar), la participación activa del Notario en el acto. Como expresa Zinny, "el alto grado de objetividad y reducido margen de error que la fe pública reclama, sólo se alcanzan cuando la percepción del Notario se logra..intersensorialmente, por el conducto de ambos" (el Notario les lee, les oye decir sí, ve a las partes además asentir con el gesto, con su expresión total, la suscripción, la entrega y recuento del dinero, de las llaves, etc.) comprobando la autenticidad del acto.

Para el Derecho anglosajón y también para el de Estados Unidos de Norteamérica, la noción de contrato es diferente de la del Derecho continental europeo; en ellos, el contrato es el resultado de un intercambio de promesas que dan derecho a exigir el cumplimiento judicial de las mismas. Como expresa Juan M. Farina "en el "common law" una promesa sólo es sancionada (enforceable) en cuanto revista la forma del "act under seal", o exista una "consideration", es decir, en este último caso, en cuanto forme parte de un negocio de cambio....Lo que cuenta es la voluntad del promitente, en cuanto que promete exigiendo a su vez algo al promisario, y no la justificación extracontractual del beneficio o del sacrificio."

Como expresa Couture "la escritura, en sí misma, es la representación de una representación; la representación a cargo del escribano de la representación a cargo de las partes de sus recíprocos estados de voluntad. Es una representación de ciencia, de una representación de voluntad." Según Saussure el lenguaje " es una forma, no una sustancia" y el documento, más allá de su función, es un soporte del lenguaje escrito que ha sido y puede modificarse a través de los tiempos, aún en el caso de los "documentos constitutivos", en los que el documento da el ser al negocio y, en la actualidad, según Cariota Ferrara, en términos generales, "la forma, en contratos y negocios jurídicos, es la forma de la declaración de voluntad."

El actual documento electrónico contiene un mensaje de texto alfanumérico (o diseño o gráfico) en un lenguaje convencional (el de los bytes) sobre un soporte material (cintas o discos magnéticos o memorias en circuito) destinado a durar en el tiempo (en modo diverso según se trate de memorias de masas, volátiles, Rom o Ram). Puede ser considerada escritura, la manifestación material de cualquier lenguaje natural o convencional , siendo los bytes las unidades de lenguaje de los documentos electrónicos, representativas de las palabras del texto escrito en cualquier idioma.

Muchos contratos se realizan hoy en día en forma oral, y aún entre los que se realizan por escrito, existe una amplia diversidad de formas, siendo sólo una parte de ellos los que necesariamente tienen como requisito de validez la escritura y aún menos los que requieren escritura pública, aún cuando tales exigencias se relacionan en general con la importancia que el ordenamiento jurídico adjudica a los bienes a que se refieren. .

III – OBLIGACIONES PACTADAS POR MEDIO DE ODENADORES

"La masa documental que requería ejércitos de personal, espacios sin fin y procesamiento". Expresan Kleidermacher y Aguinis- "justificó el calificativo de tiranía del papel que se utilizó para este siglo, dominado por el atavismo documental. La computación, entonces, importa la liberación de tal opresión. Hoy un microprocesador medio, personal, posee capacidad de memoria expandible sin límite y puede interconectarse a sistemas internacionales, leyendo las noticias a medida que se producen en todo el mundo en forma directa como si estuviera en Nueva York, París, Tokio y Buenos Aires, al mismo tiempo".

Cuando la obligación se pacta a través de una computadora las partes no están simultáneamente presentes en el mismo espacio, efectuándose las expresiones de voluntad a través de la red informática, lo que desdobla el acto simultáneo del otorgamiento. En realidad, también en la forma papel la simultaneidad en cierta manera es una ficción, ya que nunca las partes consienten exactamente al mismo tiempo, ni aún en el caso de escritura pública, pero la presencia simultánea de las partes en un lugar, día y hora determinados y el asentimiento más o menos simultáneo de las obligaciones asumidas, reducen el período de tiempo al mínimo, de tal manera que permiten razonablemente ignorar tales lapsos de tiempo. En las obligaciones asumidas a través de la red el procesamiento por medio de ordenadores permite observar las diferentes secuencias.

El uso de los ordenadores en las transacciones nacionales e internacionales, requiere una regulación desde el punto de vista de la contratación; constituye un nuevo modo de contratar que se basa en mensajes emitidos y recibidos, con claves, códigos y sistemas de estaciones de interconexión y redes, con registro de las operaciones en las memorias de cada equipo. No hay papel que contenga el contrato con las firmas de las partes, que lo realizan "entre ausentes" ya que la aceptación no es dada en presencia de la otra parte; el consentimiento se rige por las reglas del regulado para los contratos por medio de agentes o correspondencia epistolar o telegráfica; suministrados los actos al ordenador, éste puede conservarlos en la memoria hasta que sean utilizados y realizar distintos procesos con ellos hasta darles salida o emitir los resultados de los procesos realizados.

Los ordenadores se enlazan por líneas telefónicas ordinarias mediante un "modem" en cada extremo receptor que convierte los dígitos binarios del ordenador en canal de señales que pueden trasmitirse por los hilos telefónicos, pudiendo comunicarse entre distintos países a través de satélites de comunicaciones situados a gran distancia de la tierra, que son los que transmitirían los datos del ordenador. El computador viene a desarrollar un rol similar al de los medios de comunicación tradicionales: telegramas, telex, fax, etc.-

Se señalan como características de los contratos celebrados por medios informáticos: la falta de documento escrito, la inexistencia de relación directa entre los contratantes, que dificulta la individualización de los sujetos intervinientes por lo que no es apto para contratos en que es relevante la persona contratante y que la oferta debe limitarse a bienes fungibles, perfectamente individualizables mediante descripción a distancia de su especie y calidad.

Se plantean pues dos tipos de cuestiones nuevas a resolver: 1) por un lado las relativas a la expresión de la voluntad a través del medio informático, que incluye el problema de la identificación de los contratantes y el relativo al

contenido de la declaración y a la formación de la voluntad y 2) por otro, dada la transmisión de esa voluntad a través de la red, las cuestiones que se refieren al momento en que nace la obligación, es decir, en qué momento el consentimiento es obligatorio, los problemas que afectan a la seguridad en el tráfico jurídico de bienes, al nuevo lenguaje y las reglas de interpretación , así como al contenido de las obligaciones . En estos últimos puntos el tema se conecta con los cambios producidos en la contratación, que unidos a los cambios provocados por la tecnología informática, provocan un desequilibrio entre las partes contratantes, que afecta los principios rectores del Derecho especialmente en cuanto a la equidad. A efectos de amortiguar tales efectos o reconducir tales situaciones de hecho hacia la impresindible legitimación del sistema mundial en aras de su propia conservación, han surgido especialmente en las áreas más desarrolladas del sistema, conceptos y legislaciones tendientes a tales efectos.-

III.1.1 Identificación de los contratantes.-

En cuanto a la identificación del usuario existen dificultades debido a la inseguridad de los instrumentos técnicos: las tarjetas magnéticas al portador, pueden ser utilizadas por persona distinta del titular, las claves magnéticas, pueden ser reproducidas, el número de código puede ser utilizado por otra persona, igual que la palabra de orden; el timbre de voz se está utilizando combinado con otro sistema de identificación, usando palabras o frases que se cambian de tanto en tanto, la impresión digital transmitida a través del computador o el reconocimiento y memorización de la firma del usuario a través del ordenador. La conclusión es que el uso combinado de estos sistemas puede otorgar un grado de certeza en el control de la identidad del emisor del mensaje, mayor que la que da la firma autógrafa.

III.1.2 Contenido de la declaración.-

En cuanto al contenido de la declaración, sólo puede obtenerse el uso de un soporte que sufra una transformación irreversible en el momento de su utilización. Según D´Aglio, "el soporte óptico (del tipo de "compact disc") o el mecánico (tarjeta perforada) o el fotosensible (tipo microfilm) sufren con el uso una transformación irreversible y son idóneos para garantizar el contenido de una declaración. En cambio el soporte magnético excluye el carácter de indelebilidad de la escritura, por lo que habrá que recurrir a otros medios técnicos para evitar la alteración del contenido de la declaración. Uno de ellos puede consistir en un sello electrónico que impide las correcciones o modificaciones del contenido, luego que la escritura ha sido "sellada".

El documento electrónico debe brindar las mismas o similares garantías de seguridad que el soporte papel, para servir de asiento a las obligaciones contraídas, lo que lleva a la consideración de cómo la manifestación de voluntad se expresa a través de estos medios informáticos.

En una contratación entre dos particulares, el procedimiento se reduce al tecleado de determinadas opciones en la máquina; lo que nos interesa desde el punto de vista del derecho es si la obligación asumida a través de estos medios es válida produce los mismos efectos que en la contratación a través del soporte papel: en términos generales tal manifestación de voluntad tiene la misma validez que la realizada en soporte papel y con similares requisitos y condiciones en cuanto al fondo, (consentimiento libre, no dado por error, violencia o dolo, etc.) siendo la problemática de la forma de expresión, la firma digital y la contratación electrónica, punto que es objeto de otro subtema (2.4).-

Aquí se ve la necesidad de que el usuario que utiliza directamente este medio para pactar obligaciones debe tener conocimiento del funcionamiento de los sistemas informáticos, para no incurrir en consentimiento erróneo por ignorar la técnica que está empleando y también tener clara conciencia de que las obligaciones que asuma por este medio tienen igual validez y efectos que las asumidas a través del soporte papel: una obligación asumida a través de medios informáticos tendrá las consecuencias relativas a su cumplimiento o incumplimiento, eficacia, prueba, etc., establecidas en las disposiciones legales que rigen para dichas obligaciones en general, sin discriminación del soporte utilizado.

En las obligaciones pactadas a través de estos medios, referentes a bienes inmuebles o a determinado tipo de

bienes muebles de mayor importancia, establecido según el criterio de los distintos países, será necesario otro tipo de formalidades que incluyan la actividad notarial, para la protección del individuo o persona jurídica que contrae tales obligaciones y de sus derechos, mediante sistemas de claves públicas y privadas, autoridades certificantes, sistemas de verificación, encriptado de los mensajes que como la Organización española FESTE, integrada por el Colegio Nacional de Notarios, el Colegio Nacional de Corredores de Comercio, la Universidad de Zaragoza, el Consejo General de la Abogacía de España, L universidad de las Islas Baleares y la empresa Inter Computer, así como Notarios que voluntariamente quieren incorporarse a dicha Institución, aporten control de seguridad a la red, que de expandirse a nivel internacional, consistiría en una cadena de seguridades integrada por estas organizaciones nacionales .

En E.E.U.U. , según Mauricio Devoto, se ha creado una red de autoridades certificantes a nivel de empresas comerciales privadas; una de las dos primeras empresas que han obtenido licencia en el Estado de Utah para realizar tal actividad, Arkanus, ha incorporado la figura del "Crypto Notary" como autoridad de registración; en el "Notaries Public Reform Act Utah Code" el mensaje electrónico o documento se considera completo si la firma digital fue puesta en presencia del notario y éste confirmó que el signo digital es verificable pro la clave pública y pertenece al emisor del mensaje o documento; la Asociación de Abogados de los Estados Unidos (ABA: American Bar Asotiation), ha creado la figura del "Cripto Notary" como oficial de seguridad en el comercio electrónico, que combina la experiencia técnica y la legal y tendría competencia para intervenir en transacciones dentro de una escala muy amplia, que requiere diferentes tipos de seguridad según la clase de transacción de que se trate; en el proyecto de ley española de firma electrónica, según informe de la Universidad de Zaragoza de julio de 1998 se consideraría legitimación de firma electrónica la aseveración de Notario o Corredor de Comercio de que dicha firma ha sido puesta o reconocida en presencia del mismo por su titular y en el caso de declaración de voluntad transmitida telemáticamente por Notario o Corredor y firmado electrónicamente por éstos tendría iguales efectos jurídicos que los documentos escritos de la misma clase; en el Reglamento italiano se reconoce el testimonio de Notario u otro oficial público autorizado atestiguando que la firma fue puesta en su presencia, previa acreditación de identidad, de validez de la clave utilizada y de que el documento responde a la voluntad de la parte y es lícito.

III.1.3.Formación de la voluntad.

El empleo del computador puede incidir directamente en el proceso de formación de la voluntad negocial. Como lo ejemplifica D' Aglio, un empresario puede programar el ordenador de manera que sólo acepte pedidos recibidos cuanto éstos cumplan determinadas condiciones: a) que el precio de la oferta sea igual o superior al pretendido por el empresario y b) que la cantidad demandada sea igual o menor a la existente; cuando el computador recibe una propuesta contractual, confronta cantidad y precio con los datos memorizados y accede a la propuesta según lo previamente establecido y mediante los datos recibidos; en este caso el computador actúa como instrumento de elaboración de la voluntad individual y además transmite esa voluntad negocial; actúa en forma autónoma, aunque siguiendo instrucciones y procedimientos, acepta la operación comercial propuesta transmitiendo al otro contratante la declaración negocial, prevee cierto número de variantes sobre las que puede reunirse la concreta voluntad negocial. La programación del ordenador es de por sí una manifestación de voluntad ya que la voluntad negocial de la parte se encuentra en un soporte informático, en la memoria del computador, con las variables que se le ordenan, fijando condiciones o plazos. Esa información que contiene la máquina es reconocida por el destinatario a través de determinados procedimientos, según fue programado. Así, el ordenador es además instrumento de encuentro de diversas voluntades, correspondientes a sujetos distintos; según esté programado, selecciona la oferta memorizada y presenta al usuario sólo aquellas que queden comprendidas o que cumplan con los requisitos estipulados, descartando toda otra oferta pudiendo realizar una interactividad con un procesador central y delegar en el computador la selección de la oferta que interesa al usuario.

III.2.1 Momento en el que nacen las obligaciones.

En el Derecho uruguayo es de aplicación el artículo 1265 del Código Civil que establece que "El contrato ajustado por mensajero o por correspondencia epistolar o telegráfica, se perfecciona en el lugar y en el acto en que la respuesta del que aceptó el negocio llega al proponente.", siguiendo el criterio del momento y lugar en que el

proponente recepciona la aceptación, tomando en cuenta el conocimiento que de tal aceptación realiza el proponente como forma de fijar el momento en que ambas partes conocen que la contraparte está de acuerdo con el pacto negocial.

Nuestro Código civil regula con bastante precisión los contratos a distancia en cuanto al consentimiento y demás requisitos, así como contemplando diferentes situaciones de hecho: fija hasta qué momento el proponente está en libertad de retractarse de la propuesta (hasta que la respuesta del que aceptó llega al proponente), el compromiso de esperar la contestación y no disponer del objeto del contrato hasta después de desechada la oferta o hasta que hubiere expirado el plazo determinado (art.1265 in fine), la libertad que tiene el que acepta el negocio, similar a la del oferente, prevee el caso de respuesta tardía y sus efectos, establece plazo para considerar tardía una respuesta (24 horas viviendo en la misma ciudad y 30 días "desde que haya transcurrido el tiempo necesario para que las dos comunicaciones llegaran a su destino" en caso de tratarse de otros lugares (art.266), se prevé el caso de modificaciones de la propuesta y los efectos de dichas modificaciones (art.1267).- El Código Civil argentino establece que "La forma de los contratos entre presentes será juzgada por las leyes y usos del lugar en que se han concluido" (art.1180 CC). El problema se plantea cuando se trata de contratos internacionales; en cuanto a determinar cuál es el lugar donde se plasman ambas voluntades, de las que surge el vínculo contractual, puede entenderse que lo es donde se emite la aceptación, pero sería necesario que tal criterio se adoptara en una normativa global a todo el sistema. El Tratado de Derecho Civil Internacional de 1889 establece que "La ley del lugar donde los contratos deben cumplirse decide si es necesario que se hagan por escrito y la calidad del documento correspondiente" (art.32) así como su existencia, naturaleza, validez, efectos, consecuencias y ejecución..." En suma, todo cuanto concierne a los contratos bajo cualquier aspecto que sea"(art.33.) En el Tratado de Derecho Civil Internacional de 1942 se establece que "La perfección de los contratos celebrados por correspondencia o por mandatario, se rige por la ley del lugar del cual partió la oferta aceptada", estableciendo pues un criterio diferente. El tema tiene relación con la unidad de acto que se requiere en principio para los documentos notariales, pero tal unidad de acto negocial que en los contratos a distancia se ve afectada en cuanto al espacio, tiene su fundamento en la oralidad originaria de las formalidades contractuales del sistema latino, en el Imperio romano, siendo la inmediación de las partes necesaria para la expresión y recepción de los "verba", las palabras constitutivas del contrato, que no podían ser oídas por la otra parte ni por el tabelio, si no era en un acto único, de sujetos simultáneamente presentes situación para la que los medios informáticos ofrecen unas solución adecuada que facilita la realización material de las negociaciones a distancia, brindándoles al mismo tiempo una garantía técnica que, unida a la técnica jurídica notarial, puede brindar el mayor nivel de seguridad y agilidad de todos los tiempos.

Como expresó la Escribana María Wonsiak en el III Congreso Notarial del Mercosur realizado en Punta del Este, (Uruguay) en 1997 refiriéndose a la legalización de documentos provenientes del extranjero"_ la labor asesora del Escribano en estas circunstancias me parece sustancial. Justamente por la diferencia legislativa es sumamente importante que los Notarios estemos en condiciones de conocer las diferencias y de asesorar a las partes contratantes para que tomen los recaudos según las negociaciones y, en su leal saber y entender, según las circunstancias de cada una de ellas. En absoluto uso de la autonomía de la voluntad, debemos recordar la importancia que tienen los acuerdos sobre valor probatorio cuando se decide recurrir a la contratación electrónica para los negocios."

Siendo el Notario portador del "derecho de documentar", por ejercer una función pública (en el Uruguay, de ejercicio privado), por delegación estatal, sometido a responsabilidades profesionales, civiles y penales estrictas, portador de la fe pública estatal, su función en el campo de las obligaciones pactadas a través de medios informáticos se torna imprescindible como garantía de justicia cautelar, en prevención de litigios, guardián de la paz jurídica, esencial para la seguridad en el tráfico jurídico de bienes. El hecho es reconocido por las empresas comerciales como la mencionada Arkanus y otras así como por las demás organizaciones ya mencionadas. Como expresa el Notario español Rafael Gómez Ferrer, la colaboración internotarial resultará absolutamente conveniente y muy necesaria entre notarios de distintos países con el fin de ofrecer a los requirentes seguridad en sus negocios, ya que, será el aplicador de dos principios: defensa de la seguridad y la paz social y defensa de los consumidores o usuarios, en cada uno de los negocios concretos, para los que se requiera de su servicios, ejerciendo así su función de derecho preventivo o cautelar, procurando lograr el equilibrio y la equidad en el negocio obligacional pactado. En el caso de obligaciones acordadas a distancia, a través de fax o modem u otro medio telemático, el mecanismo formal de las escrituras públicas y de las actas notariales en su caso, puede acreditar en forma fehaciente, en cada extremo de la red, a través de distintos notarios, la existencia de los hechos y documentos, incluso reafirmar la identi-

ficación de los otorgantes, uniendo la seguridad jurídica a la seguridad material de la transmisión por el sistema informático, separándose las declaraciones en el espacio, como en el derecho germánico antiguo, o a similitud del derecho anglosajón, en cuanto a las promesas obligacionales.

De ahí la importancia especial que en materia de obligaciones adquiere la adopción de la informática como lenguaje y su relacionamiento con los requisitos esenciales para la validez de una de las fuentes de las obligaciones como es el contrato. En el ámbito de las obligaciones pactadas por medios informáticos, el nuevo medio de expresión de la voluntad, debe cubrir requisitos precisos que garanticen la emisión y recepción de los mensajes, a efectos de obtener un consentimiento válido.

Los problemas continúan siendo los mismos: la certeza respecto a la autoría de la expresión de voluntad negocial, la alterabilidad del documento, la configuración de los textos a través de diferentes herramientas y en distintos materiales, hoy en las computadoras. Es a través de un proceso histórico que se ha llegado a la documentación escrita, tal como la observamos hoy en día, en etapa de tránsito hacia la documentación electrónica.

III.2.2- Seguridad Jurídica y Seguridad Informática.-

En las obligaciones pactadas a través de las redes informáticas es necesario desarrollar la aplicación de técnicas tendientes a la obtención de la seguridad formal y sustancial. Como lo expresa el Notario español Rafael Rodríguez Adrados "Hay una seguridad anterior a la del documento, sin la cual la seguridad documental sería vana: es la seguridad sustancial", que requiere según manifiesta: 1) que el negocio sea VÁLIDO, según el ordenamiento jurídico, 2) que el documento esté redactado con CLARIDAD y SISTEMA, sin contradicciones, ambigüedades o lagunas, 3) que el negocio sea APTO PARA SATISFACER LAS FINALIDADES PRÁCTICAS que las partes persiguen, ya que las partes acuden al Notario "para conseguir sus fines lícitos y NO SOLO PARA QUE LES PROPORCIONE SEGURIDAD", 4) a través de su función el Notario coopera a la consecución de los valores superiores del ordenamiento: ante todo, la justicia, luego libertad e igualdad, por lo que debe procurar la justicia del acto o contrato contenido en el documento. El contrato cumple su misión anticonflictiva si no surge de él un contencioso."

El nuevo medio a través del cual se pactan las obligaciones, debe pues cumplir tales requisitos de seguridad, a cuyos efectos el Derecho debe prever que por el hecho de la utilización de tales medios, no se pierda la seguridad sustancial y formal lograda hasta el presente.

En este punto debemos destacar que la intervención del Notario en la documentación, brinda al usuario la seguridad jurídica formal, (en cuanto al hecho del otorgamiento, la fecha y la identidad de los otorgantes) y de contenido, tratándose de escrituras públicas; seguridad en cuanto a su legalidad y a la fecha de su incorporación a los Registros de Protocolizaciones si se trata de documentos que ingresan al mismo y certificados que emite. Pero además, y sobre todo con relación a las obligaciones pactadas a través de estos medios informáticos, se acentúa la importancia de las funciones asesora y formativa de la voluntad de las partes.-

III.2.3 Seguridad Sustancial: Contenido de las Obligaciones a través de los Medios Informáticos.-

Las obligaciones, en su esencia, no se ven afectadas por el nuevo soporte que las contiene; no se agrega item alguno al "dar, hacer o no hacer", y continúan regladas por las normas sustanciales del Derecho Civil y Comercial. Tampoco se modifican las normas relativas a la capacidad, consentimiento, causa u objeto, (requisitos esenciales de validez), efectos jurídicos o reglas de interpretación, tipos contractuales, caracteres de cada uno de ellos y de las obligaciones que de los mismos emergen.

En las obligaciones que surgen de contratos consensuales, relativas a bienes muebles, el pacto se realiza en general en forma verbal o por documentación privada entre las partes, salvo en el caso de determinado tipo de bienes muebles, (automotores por ejemplo) o universalidades (ej: establecimientos comerciales) para los que se esta-

blece un sistema de Registro de la Propiedad mueble o de Comercio, respectivamente, a efectos de oponibilidad frente a terceros. En las obligaciones emergentes de contratos reales el documento sirve de título hábil para ejercer el derecho real que en el mismo se reconoce (dominio, hipoteca, prenda) existiendo en los contratos solemnes la exigencia del cumplimiento de las solemnidades (escritura pública para la enajenación de inmuebles). Los nuevos medios afectarían no la existencia ni la validez misma del acuerdo obligacional, ni las obligaciones en sí mismas, sino la forma de expresar el consentimiento, constituyendo cuestiones relativas a la prueba de las obligaciones y no a éstas en sí mismas.

Como expresa el Escribano uruguayo Gerardo Caffera: "Simplemente se presenta una nueva forma de almacenar signos representativos de manifestaciones volitivas negociales y un nuevo canal a través del cual fluirá la declaración negocial (propuesta y aceptación). Si bien la forma "real" de los componentes de la declaración no es idéntica a la "visible", ello no es demasiado novedoso: tampoco lo era en una transmisión telegráfica en la época de la sanción del Código Civil. Sin embargo en uno u otro caso la lectura puede realizarse en cualquiera de los planos: el poco "amigable" Código Morse, o el poquísimo amigable lenguaje de los bytes, por un lado, y el resultante de la "interfase" correspondiente por el otro."

Coincidimos con Caffera en que "En sustancia esto no difiere de la operativa de los sistemas sintácticos y semántico de "cualquier"(ld) lenguaje, asociados mediante un código y pragmáticamente instrumentales en instancias de objetivación, y subsecuente transmisión de cualquier clase de estados volitivos, o informaciones."

Pero en la evolución, consideramos que este nuevo medio informático, unido al desarrollo de los contratos por adhesión y contratos en masa, productos a su vez del desarrollo económico llamado "globalización"; en los que el pacto obligacional se realiza en una relación directa entre, por una parte, cada individuo en particular y por la otra parte empresas multinacionales, poseedoras del poder económico de los saberes informáticos, del lenguaje global, con enormes bancos de datos, contribuye al amplio retroceso del principio de la autonomía privada, rector de los pactos obligacionales desde la Época Moderna y la Revolución Francesa, alterando en el actual contexto en muchos casos el principio de equidad que debe regir la contratación, y por otro lado favorece el desarrollo de una concepción del Derecho mucho más formal que sustancial.

Como forma de preservar la seguridad sustancial que el Derecho requiere, en aras de la aplicación de los principios de justicia, solidaridad y autonomía, se produce a la vez el desarrollo de otros conceptos jurídicos relativos a la protección de derechos del consumidor, derecho de habeas data, derecho a la información, cuestiones relativas a los medios publicitarios en tanto formas de distorsión de la voluntad, y el vuelco de la concepción clásica del contrato relativa a su finalidad de satisfacer intereses contrapuestos, hacia una concepción "postmodernista" de satisfacer necesidades mediante la composición de los distintos intereses de las partes. Ya se han introducido en algunos de los órdenes jurídicos de los países económico-culturalmente más desarrollados del sistema mundial primero, y se van introduciendo gradualmente en otros países, diversas normas jurídicas tendientes a aminorar los efectos que en forma más visible atentan contra los referidos principios, generando diversas fundamentaciones doctrinarias al respecto.-

III.2.4 Las Obligaciones Pactadas a través de Medios Informáticos y los Contratos en masa o en serie.

Las grandes empresas mercantiles, industriales y/o financieras, ante la imposibilidad de formalizar contratos singulares con cada uno de los posibles clientes, impone a éstos un contrato tipo previamente redactado, y en el que el Estado suele establecer ciertos límites o predisponer cláusulas en amparo del público. El contrato ya no es la obra común de ambas partes sino que una de ellas (el cliente) se limita a aceptar o rechazar el único contrato posible, no existiendo igualdad entre las partes, no existiendo en ellos ofertas ni contraofertas o regateo, dada la dinámica mercantil prescindiéndose de la consideración de situaciones individuales, en búsqueda de mayor celeridad y seguridad para el empresario, debiéndose recurrir a las normas del derecho civil y a los principios subyacentes que permiten reequilibrar el negocio. (derechos del consumidor, cláusulas limitativas de rescisión posible, etc.) En el juego de presiones y contrapresiones la contratación en masa, sobre cláusulas predispuestas, y las "condiciones generales".de contratación impuestas por el empresario, hace que si bien la esencia del contrato no cambia, como

expresa López de Zavalía, se hace necesario establecer limitaciones para que rija el principio de justicia; lo que está en crisis son las ideas sobre el contrato.

A tales efectos la función asesora y formativa de la voluntad del individuo que ejerce el Notario Latino, por la esencia de su función, resulta imprescindible, como garantía de la seguridad sustancial, en las obligaciones que se contraen a través de los medios informáticos, apoyada por la legislación decuada que tienda a restablecer el equilibrio.

III.2.5 Obligaciones pactadas a través de Medios Informáticos y nuevo lenguaje.-

Las obligaciones pactadas a distancia generan un nuevo lenguaje que debe ser común y requiere determinadas precauciones tendientes a preservar el contenido de las obligaciones, que contemplen las características especiales del mismo, como sucede en el caso de otorgantes que desconocen el idioma en que se redacta el documento, (español, en el caso de Uruguay), caso en que se utilizan testigos que conozcan el idioma del otorgante el español a la vez y, para el caso de que el acto requiera de la presencia del Notario, se exige que éste también conozca el idioma del otorgante además del español español por supuesto. La finalidad en ambos casos es que el consentimiento se preste sin vicios que lo invaliden y que el documento responda a la exacta voluntad tanto del obligado como del acreedor de las obligaciones acordadas. Este saber que se expresa a través del nuevo lenguaje implica desde el área de las obligaciones, que el pacto obligacional se realice a través de una comunicación libre de coerciones, basado en la igualdad y en la presuposición de condiciones universales de comprensión mutua, tendientes a la formación de un consentimiento válido, no viciado de error, expresión de la real voluntad de las partes, so pena de hacer inexigible el cumplimiento por nulidad.

Es aquí donde adquiere vital importancia la semiótica jurídica, ya que, como lo expresa Milanova Kremena, el diverso uso o sentido de las palabras y las frases en distintas áreas locales de un mismo país o entre países diferentes, puede ocasionar enormes problemas en la contratación telemática entre ausentes (no simultáneamente presentes).

Según Caffera y Mariño "El lenguaje jurídico pertenece a la clase de los lenguajes naturales. Las normas jurídicas prohiben, hacen obligatoria o permiten conductas de los hombres, creando pautas de comportamiento, por lo que, para cumplir su función deben necesariamente estar compuestas por expresiones textuales propias de los lenguajes naturales y son definibles en términos de ellas": Citan a Kalinowsky en cuanto éste "afirma que cuanto más explícitas sean las convenciones linguísticas más acentuado es el carácter artificial del lenguaje y que el lenguaje del derecho (normas jurídicas) como el de los juristas son lenguajes derivados del lenguaje natural." Y observan: "las expresiones de los lenguajes naturales son potencialmente vagas, cualquier definición que intente recoger con finalidad sus reglas de uso tendrá que recoger la imprecisión de la expresión definida. Si se desea dar a la expresión una precisión que no tiene, entonces se estará realizando una acción diferente a la atribución de significado a una expresión textual, según los usos linguísticos." De acuerdo a tal apreciación, la formación de un lenguaje común deberá basarse en definiciones precisas y definidas pero que contemplen la existencia de cierto tipo de expresiones que no tienen una traducción exacta en otros idiomas.

III.2.6 Importancia de las reglas interpretativas de las obligaciones emergentes de contratos a distancia.-

Tal situación lleva a la consideración de las reglas hermenéuticas en tal contexto global. Su contenido es más o menos similar en los Códigos Civiles derivados del Código Napoleónico; la atribución de significado a una norma que genera obligaciones, como el contrato, requiere la estricta aplicación de dichas reglas, a nuestro criterio de aplicación obligatoria, no meramente declarativas, ya que expresan en un Código las reglas a que debe ajustarse la interpretación de los textos elaborados por las partes que en uso de la autonomía privada se obligan una para con la otra o ambas recíprocamente a determinadas prestaciones.

En el actual y futuro contexto informatizado, tales reglas que establecen un conjunto de pasos y pautas para desarrollar la actividad interpretativa, son obligatorias en cuanto al orden de dicha actividad para la asignación de significado a un texto contractual y acotan la libertad del intérprete, (del juez en su caso) constituyen para el individuo que contrae obligaciones a través de medios informáticos, la garantía de aplicación de los principios de justi-

cia, autonomía y equidad frente a los centros que manejan las redes informáticas y con los cuales contrata. "Para asignar sentido al texto contractual", expresa Mariño, es preciso la elucidación del sistema de significación dentro del que se le incluye". Y la primera regla, al menos en el código Civil uruguayo, es la de la interpretación de las palabras por su "uso general, aunque el obligado pretenda que las ha entendido de otro modo", estableciendo en esta primera regla de interpretación, una metodología objetiva, independiente de la voluntad del obligado. La contratación a distancia requerirá establecer significados de uso general para los pactos de obligaciones por medios informáticos y debe quedar muy claro para cada una de las partes el significado del texto, cuáles son las obligaciones asumidas o que le son exigibles, cuáles son los límites de las mismas, cuál es el tiempo en que deben cumplirse, en suma cuáles son sus derechos y obligaciones frente a la contraparte. Encontramos en esta regla la protección del individuo frente a palabras de uso técnico que pudieren emplearse en los textos que contienen las obligaciones pactadas por medios informáticos, o que provenientes de otros países con diferentes contextos, adquieren otro significado. Es necesario pues, para interpretar las obligaciones pactadas, tener en cuenta qué significado tiene el texto para el individuo y qué capacidad de comprensión textual tiene éste, su competencia para atribuir significado al texto, estando en nuestro país fijado el límite legal en el conocimiento del individuo medio normal, al establecer el Código Civil la remisión al uso general de las palabras.

Para el caso de no poderse interpretar el haz obligacional adecuadamente, por el uso general de las palabras, como protección al individuo medio, cuando las palabras son ambiguas, debemos pasar a la segunda regla interpretativa, que se regula por una metodología subjetiva: indagar la intención común de las partes (art.1299 CCU). Estas dos reglas interpretativas de nuestro Código establecen pues un sistema que se desarrolla desde lo general a lo particular: si no es posible interpretar el contenido de las obligaciones pactadas por medio del principio general que es el del uso general de las palabras, entonces pasamos a la segunda etapa de análisis de dichas obligaciones, buscando en las palabras algo más particular: la intención común de las partes. Aquí el legislador deja de lado la consideración del uso que generalmente hacen los individuos de las palabras, para dar paso a la consideración de los individuos contratantes y a su intención común específica, abandonando así en esta segunda etapa, como expresa Mariño, la metodología objetiva para aplicar una subjetiva. Tal cambio metodológico se justifica por la finalidad intrínseca al Derecho, de resolver y abarcar los problemas generados en los hechos, ordenándolos a través de su normativa, y se pone de manifiesto en el caso, al entender que, cuando las palabras son ambiguas, o sea, que pueden interpretarse de varios modos, la regla establecida por el método objetivo carecería de eficacia, ya que no podría resolver el problema hermenéutico planteado.

Esta segunda regla nos remite a la búsqueda de la captación de la voluntad concreta de los individuos autores del texto específico que contiene las obligaciones pactadas para lo cual el intérprete (o el juez en tal calidad) debe situarse en el contexto al tiempo de celebrarse el acuerdo obligacional, debiendo tener en cuenta el momento histórico, social y cultural para luego tratar de conocer cuál fue la finalidad típica perseguida por las partes a través de ese acuerdo. La variedad de situaciones contextuales (costumbres, razas, culturas, distintas clases sociales, aún de la misma sociedad) en los diferentes países o localidades, inciden en el contenido de las obligaciones, no tanto por el medio informático en sí, sino por la posibilidad que el mismo brinda, de conectar tan diferentes individuos pertenecientes a contextos absolutamente disímiles, que pueden perseguir tan diversas finalidades e interpretar las palabras de acuerdo a infinidad de formas.

La tercera regla interpretativa indica la remisión al contexto general para el caso de cláusulas equívocas o ambiguas, lo cual en el caso de las obligaciones asumidas a través de medios informáticos adquiere importancia en relación a los diferentes contextos de las partes que realizan el pacto obligacional. Otra regla que adquiere importancia es la que se remite a los usos y costumbres del lugar del contrato ya que habrá que fijar a qué lugar se remitirá la regla en caso de usos y costumbre diferentes para cada sujeto del pacto obligacional.

Las reglas de interpretación referidas continúan en un orden cuyas pautas no corresponde exponer en su totalidad en este trabajo, pero de las que se han esbozado las primeras a efectos de aportar elementos que deberán tenerse en cuenta para una regulación adecuada de los cambios que provoca a nivel sustancial del Derecho, la transformación del medio a través del cual el mismo se expresa. Este es en esencia el problema de la comunicación en sistemas globales y abarcativos de diversas culturas, que se refleja en las obligaciones pactadas a través de medios informáticos. Tales problemas se deben resolver sobre la base de un sistema global de definiciones generales

y marcos comprensivos bajo principios de tolerancia, solidaridad, autonomía y justicia, para enriquecimiento de los individuos que participan en él para la permanencia del mismo. Concluímos que si se desea establecer un lenguaje jurídico universal, por otra parte necesario, mediante definiciones claras y precisas se deberá tener en cuenta como determinantes tales principios, a efectos de lograr el pacífico cumplimiento y asunción de las respectivas responsabilidades generadas por las obligaciones pactadas, como base de la necesaria estabilidad de tal sistema.

III.2.7 Situación de riesgos y obligaciones pactadas a través de medios informáticos.

Desde el punto de vista de los riesgos la innovación que introduce la informática en la forma de expresión de la voluntad y el consentimiento cambia determinado tipo de riesgos (falsificación documental, de firmas, etc.) regulados por determinadas normas jurídicas típicas, que expresan un comportamiento adecuado a ellas y una sanción al comportamiento inadecuado a las mismas, ofreciendo un sistema de seguridad formal y sustancial que el individuo medio conoce o está en condiciones de conocer a través del asesoramiento del Notario interviniente en la contratación, en cuanto compete a éste el ejercicio de la función asesora y formativa de la voluntad (Carnelutti). La aplicación de la informática a los pactos obligacionales introduce otro tipo de riesgos inherentes al nuevo medio que deberán ser previstos con relación a las nociones de cumplimiento o incumplimiento de las obligaciones pactadas, teniendo en cuenta que el nuevo saber, por tratarse de un saber especializado, constituye un conocimiento que implica la mayor responsabilidad de quien detenta el "poder del saber" y al mismo a tiempo afecta las posibilidades de cumplimiento de los pactos.

Esto es notorio sobre todo en el actual contexto de proceso de cambio en el que la mayoría de las personas aún no conocen el funcionamiento de la red informática a través de la cual contratan; la seguridad queda basada en la confianza que esas personas depositan en el sistema, como sucede en el caso de la contratación referente a tarjetas de crédito o la misma contratación que realiza el individuo aislado con el sistema bancario o financiero.- Aún no está estructurado el sistema que relaciona las responsabilidades del operador jurídico y del operador informático en esta situación y tampoco está munido el jurista de los conocimientos adecuados para asumir esa responsabilidad. Será necesario pues incorporar el conocimiento de la informática a los estudios jurídicos, especialmente a los notariales, en cuanto es a través de los contratos en los que éste interviene en el ejercicio de su función pública, (en nuestro país, de ejercicio privado) asesora, formativa y autenticante de la voluntad, que se pacta gran cantidad de obligaciones relativas a bienes inmuebles y muebles, en algunos casos, por disposición legal, en otros, por voluntaria decisión de las partes.-

La enorme cantidad de datos que permite incorporar el saber informático, apareja un "poder del saber" frente al cual el individuo que contrata en forma aislada con las organizaciones que manejan tales conocimientos, se encuentra indefenso, debiendo basar la seguridad en las negociaciones que realiza, en el principio de confianza, hecho del que surge la necesidad de adecuar a este sistema las nociones de cumplimiento o incumplimiento de las obligaciones.-

III.2.8 Nociones cumplimiento o incumplimiento de las obligaciones con relación a las obligaciones pactadas por medios informáticos.-

"Mientras en las obligaciones de medios el incumplimiento se constata por la contrastación de la conducta realizada por el sujeto obligado con el módulo abstracto de la diligencia del buen padre de familia, en las obligaciones de resultado se constata por el solo hecho de la no obtención del resultado material", como sintetizan Gerardo Caffera y Andrés Mariño (*).

Con relación a las obligaciones pactadas a través de redes informáticas, para cumplir con los principios de equidad y justicia del Derecho, será necesario estudiar el texto y el contexto particular de los contratantes, sus posibilidades de acceso al saber informático suficiente o de obtener el asesoramiento necesario para poder configurar un real consentimiento, a efectos de constatar en qué casos se produce o no el incumplimiento.

El diferente sentido de las palabras en contextos socio-culturales distintos, hace necesario estudiar y definir

muy adecuadamente cuál es para cada contratante la "diligencia media" o la de un "buen padre de familia", cuando como por ejemplo en nuestro Código dicho comportamiento se establece como eximente de la culpa; el mismo concepto de culpa, debe ser también objeto de estudio y definición, ya que, si la claridad de los pactos obligacionales sólo lo es para una de las partes y no para otra, podría estarse violando el principio de equidad en la contratación, por diferentes interpretaciones de los términos contractuales generadores de esas obligaciones . El nuevo medio introduce un elemento formal en el que el saber informático de los contratantes afecta en forma decisiva las posibilidades de cumplimiento de los pactos, pudiendo incidir como eximente de responsabilidad, en el caso de las obligaciones de medio, probada la diligencia media o de un buen padre de familia, dando lugar a la liberación del deudor en cuanto al cumplimiento de su obligación. En el caso de las obligaciones de resultado, la ignorancia en cuanto al medio informático utilizado podría dar lugar también a eximente en el caso de asumirse una obligación que pudiera considerarse imposible de cumplir.

III.2.9 Las obligaciones en derecho comercial y la informática

El derecho de contratos comerciales se ha desarrollado en los usos y costumbres mercantiles, diversificándose y especializándose, dando nacimiento a una nueva realidad; los contratos de adhesión, que constituyen la regla en el tráfico comercial, el contrato no negociado. La mayoría de los contratos comerciales se celebra en alguna de estas modalidades: contratos formulario, condiciones generales de contratación, contrato de adhesión, contrato normado, contrato de ventanilla, contratos no paritarios, oferta no negociable, contratos no negociados de modo absoluto o de modo relativo. Este comportamiento consuetudinario pone de manifiesto que no todo el derecho se encuentra en el derecho escrito, sino que existe un derecho viviente, que se asienta en la costumbre, como expresa Rezzónico.

Este hecho se basa en que el Estado no tiene la posibilidad de dictar leyes que cubran todos y cada uno de los aspectos de la conducta humana. La lex mercatoria o ius mercatorum, como costumbre en el derecho mercantil, nació en el medievo; la autonomía de la voluntad o autonomía privada, ámbito del protagonismo empresarial en que los entes económicos van creando sus propias reglas autónomas de comportamiento, integradoras de la nueva "lex mercatoria", nació de circunstancia similares a las que dieron origen a la "lex mercatoria" del medievo: después de la segunda guerra mundial, el reconocimiento de la lex mercatoria sobre todo en el comercio internacional se apoya en la consideración del consenso común como regla vinculante de la conducta humana, fuente creadora de derecho.

Los usos y costumbres no pueden crear derechos sino cuando las leyes se refieran a ellos o en situaciones no regladas legalmente (CC argentino, art.17, similar CCU) El Código de comercio argentino se refiere a la costumbre como fuente de derecho para casos no reglados. En la medida que surjan estas nuevas reglas es que a través de la aplicación de la legislación podrán controlarse los excesos de aplicación del principio de autonomía privada, como se observa en algunas legislaciones sobre derechos del consumidor y, en el caso de la informática, el pacto realizado a través de esta tecnología requiere garantías para el usuario individual, entre otras, la posibilidad de conocer exactamente los límites obligacionales que pacta, así como el derecho de habeas data, etc.- mediante los "medios informáticos" o por lo menos utilizarán este medio para su concreción en alguna de las etapas del pacto. Pero además esto se une a otras características del cambio global, como es la de la realización de contratos en masa. Para el individuo aislado que contrata a través de la red, es ésta quien le aporta la seguridad en la contratación y quienes conocen y manejan la red. Esto genera nuevas situaciones de hecho, como algunas ya planteadas, en cuanto al derecho de fondo, que producen todo el derecho de protección a ese individuo que se obliga o se constituye en acreedor del cumplimiento de obligaciones a través de contratos de adhesión transformando la contratación de individuo con individuo o con determinados conjuntos conocidos de personas, en una multiplicidad de contratos y acuerdos realizados por ese individuo que contrata en forma aislada, totalmente conocido y detectado a través de las redes informáticas, mediante bancos de datos que contienen desde la información más simple (documento de identificación, domicilios actuales y anteriores, estado civil, nacionalidad, etc.) hasta otra que incluye actividades, expresiones, costumbres, hábitos de consumo, etc., dando un perfil de su personalidad total y permitiendo incluso proyecciones de actitudes y comportamientos a futuro. Tal conocimiento permite desde quienes lo detentan, un manejo casi total de cada uno de los individuos, a través de estímulos y otros mecanismos prácticamente personalizados, que otorgan un grado de poder a los centros de saber informático, generando una potencia-

lidad de manejo de cada ser humano en particular, haciendo depender casi en forma exclusiva la aplicación de los principios éticos de quienes dirigen y tienen acceso a tales centros informatizados, y de quienes depende la estabilidad de todo el sistema global.

III.2.10 La publicidad y las obligaciones pactadas a través de medios informáticos

La moderna publicidad es otro elemento que une a las obligaciones que se asumen por medios informáticos y por cualquier otro medio, que afecta el consentimiento. Según Ghersi, la publicidad inductiva integra la relación contractual, ya que mediante la publicidad, se hace conocer bienes y servicios con la intención de generar negocios jurídicos masivos, con la metodología del contrato de adhesión o por lo menos estándar. Esta publicidad puede abarcar desde resaltar algunas cualidades hasta establecer condiciones generales o particulares de contratación. La existencia de un ordenador y un teléfono en cada hogar individual pone al alcance de la mano en forma inmediata la realización del "pacto obligacional", mediante la presión de algunos botones en el computador el teléfono. Esto genera, según Ghersi, dos problemas: el relativo a la lealtad comercial y la adhesión implícita a las condiciones generales contenidas en dicha publicidad, a veces no explícitamente.

Rezzónico estudiando la jurisprudencia al respecto, cita el fallo de un tribunal francés que resolvió una cuestión sobre el carácter obligatorio o no para el cliente, de las condiciones generales insertas en el certificado de seguro que se obtenía en un aeropuerto por medio de un "vending machine"; el tribunal tomó en cuenta que el cliente adhería antes de conocer las condiciones, sin oportunidad de leer las cláusulas, por tanto declaró inválida la estipulación por la cual la empresa se exoneraba de responsabilidad, contenida como condición negocial general.

IV RESUMEN

1- Los medios a través de los que se expresan las obligaciones han cambiado a través de la historia. Sin embargo, la finalidad siempre ha sido conferir certeza y seguridad en las negociaciones, probar su existencia, lograr la paz jurídica basada en la confianza en los diversos sistemas, más que en la fuerza coercitiva de las normas que integran el Orden jurídico.

2- El nuevo medio no difiere en sustancia de la operativa de los sistemas sintácticos y semánticos de cualquier lenguaje, asociados mediante un código y pragmáticamente instrumentales a la objetivación y trasmisión de cualquier clase de estados volitivos e informaciones.

3- 3- Las obligaciones en su esencia no cambian, nada se agrega al dar, hacer o no hacer; sin embargo, la nueva forma plantea cuestiones relativas a la identificación de los contratantes, a la expresión de la voluntad, al contenido de la declaración, al momento en que nacen las obligaciones.

4- Asimismo, la posibilidad de realizar contratos a distancia genera problemas relativos al lenguaje utilizado, en cuanto a la interpretación de las palabras en distintos contextos socio-culturales, que requerirá la aplicación de reglas hermenéuticas adecuadas a tal realidad global, para el logro de los principios del Derecho.

5- El nuevo medio constituye además una nueva variable a tener en cuenta en las obligaciones, con relación a la clasificación en obligaciones de medio y de resultado, al concepto de culpa, al cumplimiento o incumplimiento de las mismas.

6- Estos cambios, unidos a los producidos en las formas de contratación, en cuanto se da en éstas la contratación en masa o en serie, los contratos de adhesión, la aplicación de la "lex mercatoria", de las cláusulas predispuestas y "condiciones generales", con la incidencia además de la publicidad en el acto volitivo, como parte de la negociación, provocan una situación de hecho en la cual el desequilibrio entre las partes contratantes, por un lado el individuo aislado y por otro las grandes empresas transnacionales, comerciales, industriales o financieras, poseedoras del poder económico y del poder del saber, en el caso del saber informático, afecta la equidad del contrato y los principios rectores del Derecho.

7- Tal situación provoca el desarrollo de doctrinas y legislación tendientes a paliar o reconducir esa realidad hacia el cumplimiento de los fines del Derecho: los principios de justicia, solidaridad, equidad. En tal sentido se torna imprescindible la función formativa y asesora del Notario, y en cuanto a la informática, la aplicación de los derechos de habeas data, derecho al consentimiento informado, derecho de retracto, entre otros, como forma de preservar los derechos humanos de los sujetos particulares y la propia estabilidad de un sistema mundial que necesariamente debe basarse en la confianza para su propia permanencia como tal.

BIBLIOGRAFIA:

ACQUARONE, María.- Perspectiva de la función notarial frente al nuevo orden internacional. VI Jornada Notarial Iberoamericana.-

AVILES GARCÍA, Javier: Cláusulas abusivas, buena fe y reformas del derecho de la contratación en España. Revista de Derecho Inmobiliario. (España. Pag.1533 y siguientes.)

BETTI, Emilio. Teoría General del Negocio Jurídico. (En especial: Cap. VI: Interpretación del Negocio Jurídico)

COUTURE: Diccionario Jurídico. Montevideo, Uruguay.-

CARNELUTTI, Francesco: La figura jurídica del Notario. Rev. Internacional del Notariado Latino. Año 1950-.

CAFFERA, Gerardo: Una mirada a los contratos informáticos al tema del consentimiento por medios electrónicos. Anuario de Derecho Civil Uruguayo. Tomo 26

CAFFERA, Gerardo: Las obligaciones de resultado: un paradigma en crisis. Anuario de derecho civil uruguayo. Tomo 28.1998

CURBELO SORIA, Carmelo y otros: Nuevas normas jurídicas en materia informática.

DE LA FUENTE, Juan Angel: Conferencia sobre Derecho Informático: Conferencia en Asociación de Escribanos del Uruguay. 1998

DEVOTO, Mauricio y Horacio M.Lynch: Contratación electrónica. Banca, comercio, moneda elctrónica y la firma digital: III Congreso Notarial del Mercosur .1997

DEVOTTO, Mauricio. Claves para el éxito de una infraestructura digital: la importancia de la intervención notarial en la solicitud de certificado de clave pública. (Fuente: Comisión de Derecho e Informática de la Asociación de Escribanos del Uruguay. 1999)

DELPIAZZO, Carlos: El documento electrónico frente a la integración: VI Congreso Iberoamericano de Derecho e Informática. Montevideo. Uruguay. 1998.

FARINA, Juan.- Contratos comerciales modernos.- (En especial: capítulo II: Contratación masiva, Cap. II: Concepto de Contrato- Necesidad de su revisión. Cap. IV: Responsabilidad de productores y proveedores en la contratación mercantil. Cap. V: Influencia del comercio actual) Buenos Aires. República Argentina.-

FONT BOIX, Vicente: El Notarido en los sistemas del derecho latino y anglosajón.

GALINDO, Fernando. De Aequitas a Feste. La fiabilidad de las comunicaciones electrónicas. VI Congreso Iberoamericano de Derecho e Informática. Montevideo. Uruguay, 1998.-

GHERSI, Carlos: El contrato ante las nuevas exigencias económicas sociales del nuevo milenio. Jornada de Derecho Civil en homenaje al Profesor Jorge Gamarra. Montevideo, Uruguay. 1999

GOMEZ FERRER, Rafael , Jurisdicción voluntaria. VI Jornada Notarial Iberoamericana. Quito 1993.

KLEIDERMACHER Y AGUINIS, citados por J. Farina en Contratos Comerciales...

KREMENA, Milanova, Sistemas de información jurídica al servicio de los juristas en Derecho Internacional.- VI Congreso de Derecho e Informática.

LARRAUD, Rufino: El documento notarial y su eficacia.

.MARIÑO, Andrés : La interpretación judicial del contrato en el derecho uruguayo. Anuario de Derecho Civil Uruguayo. Estudio del sistema de reglas hermenéuticas del Código Civil. T. 28

MESSINEO, Doctrina General del Contrato

MICCOLI, Mario. Derecho e Informática. Conferencia en A.E.U. Montevideo, Uruguay.- 1998

NUÑEZ LAGOS, R. Estudios sobre el valor jurídico del documento notarial. En Estudios de Derecho Notarial. T.II. España. Madrid

PETIT, Eugene: Tratado Elemental de Derecho Romano. Editorial S. Calleja. 1938

RAMOS, Federico Ernesto: Contratación electrónica. III Congreso Notarial del Mercosur. Punta del Este. Uruguay. 1997

REZZONICO, Contratos con cláusulas predispuestas.

RODRIGUEZ ADRADOS, Antonio: La persistencia histórica de la oralidad en la escritura pública. Publicación de la Real Academia de jurisprudencia y Legislación. Madrid, 1966-

SIRI, Julia: La función notarial en la economía de mercado. VIII Jornada Notarial Iberoamericana. Veracruz. 1998.-

Desafíos al Derecho Informático en el Nuevo Milenio La Protección del Derecho a la Intimidad y Privacidad frente a las Nuevas Tecnologías

RESUMEN DE LA PONENCIA

En el presente trabajo el autor analiza el desarrollo de las normas relativas al habeas data y a la protección de datos personales en Latinoamérica y propone el establecimiento de leyes de protección de datos que establezcan principios para el manejo y tratamiento de la información personal a través de normas claras siguiendo los estándares creados por las normas del Consejo de Europa, las Directrices de la Organización para la Cooperación y el Desarrollo Económico y la Directiva Europea en materia de Protección de Datos Personales.

DATOS DEL AUTOR

Pablo A. Palazzi, Argentino, Abogado, Doctor en Derecho (tesis pendiente) es Director de la Revista Derecho y Nuevas Tecnologías, Editor del Boletín Hispanoamericano de Informática y Derecho [http://www.ulpiano.com/boletin.htm] y Editor del *Boletín de Privacidad Online* [http://www.ulpiano.com/boletinprivacidad.html]
99 John Street Apt. 822 New York NY, 10038 – U.S.A.
Tel 212-706-0565 Fax 212-706-0566
pablopalazzi@yahoo.com http://www.ulpiano.com/pablopalazzi.htm

Habeas Data y Protección de Datos en Latinoamérica. Propuestas de reglamentación y armonización de estándares de protección de datos

Por Pablo A. Palazzi (Argentina)

1.- INTRODUCCION.

La presente ponencia consta de tres partes. En la primera explicamos las reformas constitucionales latinoamericanas que incluyeron el habeas data y a la legislación y jurisprudencia posteriores que han creado normas de protección de la privacidad y protección de datos personales. En la segunda explicamos porque en necesario una reglamentación *uniforme* de la protección de datos en Latinoamérica. Finalmente, sugerimos la formulación de normas de protección de datos siguiendo el modelo europeo.

En la década del setenta, tanto Europa como Estados Unidos comenzaron a preocuparse por regular el tratamiento de datos personales a través de ordenadores. Mientras que Estados Unidos adopto un modelo vertical, donde el sector publico y solo ciertos sectores privados son regulados, los países miembros de la Unión Europea siguieron adoptaron un "modelo horizontal", esto es regulando a todos los sectores por igual, estableciendo leyes de protección de datos conteniendo principios para el manejo y tratamiento de la información personal. Estas diferencias marcan los dos grandes enfoques que se han adoptado para regular la privacidad en el mundo digital.

En Europa la regulación fue posible por la existencia de normas claras: los estándares creados por las normas del Consejo de Europa, las Directrices de la Organización para la Cooperación y el Desarrollo Económico y, mas recientemente la Directiva Europa de Protección de Datos Personales. Esta directiva armoniza la legislaciones de sus países miembros y a la vez establece una valla para la trasferencia de datos a terceros países. Solo se podrá

transferir datos personales a paises que tengan una "legislación adecuada" (art. 25 de la Directiva). Esta norma es una forma de asegurar que la eficacia de la Directiva no se vea frustrada por un "paraíso informático".

2.- HABEAS DATA Y PROTECCION DE DATOS EN LATINOAMERICA.

A continuación enumeramos las normas constitucionales relativas al habeas data y protección de datos personales en Latinoamérica.

2.1.- Argentina.

El Articulo 43 de la Constitución Nacional de 1994, tercer párrafo, establece que *Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.*

La jurisprudencia argentina en materia de habeas data se ha desarrollado extensamente. Existen diversos fallos sobre el habeas data en Argentina. Existen asimismo otras normas vigentes que cumplen la función de leyes de protección de datos, y se están tratando actualmente varios proyectos de leyes sobre Protección de datos. Veamos algunas de estas normas positivas.

- Ley de Tarjetas de Crédito No. 25.065. La ley fue sancionada en el año 1998 y varios artículos fueron vetados. Pero el Congreso insistió y convirtió en ley también los artículos vetados en agosto de 1998. De especial importancia para la protección de datos es el art. 53 de la ley, que prohibe a los bancos expresamente informar a las centrales de riesgo privadas (las firmas que informan a los bancos sobre la conducta crediticia) si algún cliente de tarjeta está en situación de mora. La ley establece que los clientes morosos podrán informarse sólo al Banco Central. El articulo 53 (Prohibición de Informar) dice: "Las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias tienen prohibido informar a las bases de datos de antecedentes financieros personales sobre los Titulares y beneficiarios de extensiones de Tarjetas de Crédito u opciones cuando el Titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciacion. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina. Las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de Tarjetas de Crédito por las consecuencias de la información provista". La norma aun no fue reglamentada.

- El Banco Central ofrece la posibilidad de consultar a través de Internet sus bases de datos con información de deudas financieras. Estas son (1) Central de Deudores Consulta de deudores: usando tipo y número de documento y denominación y la (2) Base de datos de Cuentacorrentistas Inhabilitados: aquí es posible consultar por Personas Físicas, Tipo y número de documento, por Denominación Personas Jurídicas Tipo y número de documento Denominación. La consulta se realiza sobre las bases de información del Banco Central de la República Argentina conformadas por los datos recibidos de las Entidades Financieras. Un aviso en la pagina web del banco informa que "esta opción ha sido normada para consultas puntuales, no debiendo ser utilizada para descarga masiva de información. De constatarse tal situación, el B.C.R.A. se reserva el derecho de iniciar las acciones judiciales pertinentes más daños y gastos causídicos".

- Comunicación A 2729 del BCRA. Básicamente es la ultima norma relativa a la Central de Deudores del Sistema Financiero y Comunicación A 2950 del BCRA, del 16 de julio de 1999. Establece un ordenamiento de las normas del BCRA relativas al sistema financiero. El art. 8.1 de esta ultima comunicación otorga un derecho de acceso y rectificación de la información financiera contenida en esa base de datos.

La jurisprudencia sobre Habeas Data esta suplantando en parte el vacío legal que en nuestro país existe por la falta de una ley de protección de datos personales. En el caso "Urteaga" la Corte Suprema estableció que el habeas data podía usarse para acceder a información publica. En el caso "Matimport" la Corte se refirió a las facultades del registro de juicios universales para tratar datos referidos a concursos y quiebras, manteniendo su validez por cumplir fines públicos. Finalmente en el caso "Scilingo" la Corte estableció limites al gobierno. En este caso la Corte Suprema de Justicia decidió que los ciudadanos pueden utilizar la acción de hábeas data para conocer los datos que poseen sobre ellos los organismos de seguridad, los que sólo podrán negarse a suministrar la información cuando se ponga en riesgo la seguridad del Estado.

En el caso "Cadaveira" un tribunal de apelaciones sostuvo que el Estado debe proveer información veraz en el mercado y que al no hacerlo afectada la privacidad de los individuos. Y agrego que el habeas data incluía la obligación de aclarar los datos erróneos que se han comunicado a terceros, no alcanzando solo con rectificarlos. Este caso permitió a un individuo no solo corregir información inexacta sino aclarar por el mismo medio (la base de datos del Banco Central) que nunca había estado inhabilitado y que se trato de un error del banco de datos estatal. Se trata de un claro establecimiento de limites a las facultades que tiene el Estado de almacenar y tratar datos personales.

El caso mas paradigmatico en relación a las normas europeas en el sector privado es "Lascano Quintana c. Organización Veraz". Allí la Cámara Civil estableció como recaudo para el tratamiento de datos personales el consentimiento del registrado.

Por ultimo, a fines de 1999 un fallo de un juzgado civil, a través de una sentencia correctamente fundada y de gran interés para los estudiosos de la privacidad, reconoció el "derecho al olvido", incluido dentro del habeas data pero con fundamentos también en el abuso de derecho del banco de datos privado.

En cuanto a los proyectos de Leyes de Habeas Data y Protección de Datos Personales cabe consignar los siguientes: (i) Proyecto del Senador Eduardo Menem, sobre cuya base se elaboro el proyecto del Senado Nacional. Luego de un arduo debate el Proyecto de Ley de habeas Data y Protección de datos personales fue aprobado por el Senado de la Nación el 26 de noviembre de 1998. Existe actualmente una versión con modificaciones realizadas por la Cámara de Diputados. Por su parte la cámara de Diputados también elaboro un proyecto de Ley sobre base de datos de Riesgo Crediticio. Orden del Día 1441: Dictamen (con modificaciones) de las Comisiones de Comercio, de Finanzas y de Defensa del Consumidor en el proyecto de ley sobre Bases De Datos De Riesgo Crediticio. Este proyecto fue aprobado por la Cámara de Diputados pero el Senado se negó a tratarlo para evitar una duplicidad de normas (y también de trabajo).

2.2 Brasil

La Constitución de Brasil de 1998 fue la primera en legislar el Habeas Data en Latinoamérica. Tiene varias normas referidas al habeas data. Estas normas son:

- concessão (art. 5.º, LXXII)
- gratuidade (art. 5.º, LXXVII)
- julgamento em recurso ordinário; competência do Supremo Tribunal Federal (art. 102, II, a)
- mandado de segurança; direito não amparado por (art. 5.º, LXIX)
- processo e julgamento; competênciado Superior Tribunal de Justiça (art. 105, I, b)
- processo e julgamento; competência do Supremo Tribunal Federal (art. 102, I, d)
- processo e julgamento; competência dos Tribunais Regionais Federais e seus juízes (art. 108 I, c e art. 109, VIII)

- Las normas mas importantes son:

- Art. LXXII Se concederá "habeas data":

- a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;

- *Art. LXXVII son gratuitas las acciones de "habeas corpus" y "habeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.*

- *Art. 108. Es competencia de los Tribunales Regionales Federales: I procesar y juzgar, originariamente:.. c) los "mandados de seguranca" y los "habeas data" contra actos del propio Tribunal o de los jueces federales;*

A fines de 1997 se dicto la Ley reglamentaria de Habeas Data. Ley nº 9.507, del 12.11.97. (Regula o direito de acesso a informações e disciplina o rito processual do habeas data). Se refiere solo a los aspectos procesales y no trata cuestiones de protección de datos.

2.3 Chile

Hasta fines de 1999 Chile no tenia normas especificas sobre el habeas data. Su Constitución Nacional contiene normas genéricas sobre el derecho a la privacidad. El art. 19 de la Constitución asegura a todas las personas: *4. El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia. La infracción de este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley. Con todo, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan; 5. La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley...*

Pero en agosto de 1999 Chile aprobó una ley de protección de datos personales, convirtiéndose en el primer país en Latinoamérica en legislar la recopilación de datos personales. Previamente, la ley de delitos informáticos había incorporado ciertas normas protectoras de la privacidad.

2.4 Colombia

El art. 15 de la Constitución de Colombia establece que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. *De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recog ido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.* En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

En Colombia se dicto una ley sobre habeas data que la Corte Constitucional declaro inconstitucional por cuestiones formales. También hay fallos muy importantes que establecen normas jurisprudenciales sobre protección de da-

tos. Son las sentencias de unificación jurisprudencial que han establecido un derecho judicial relativo a la eliminación de los datos por el transcurso del tiempo y al consentimiento para el tratamiento de datos personales.

2.5. Nicaragua

El artículo 26 establece que toda persona tiene derecho a su vida privada y la de su familia, a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo, a respeto de su honra y reputación. Y el art. 26 punto 4 crea un derecho similar al habeas data al establecer que tiene derecho a *"A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".*

2.6. Perú

La constitución del Perú de 1994 establece en su artículo 2.- *Toda persona tiene su derecho:*

- 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con le costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria puedan levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado.

- 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afectan la intimidad personal y familiar.

- 7.Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, son perjuicio de las responsabilidades de ley. ...

- 9. A la inviolabilidad del domicilio. Nadie puede ingresar en él ni efectuar investigaciones o registros sin autorización de la persona que lo habita o sin mandato judicial, salvo flagrante delito o muy grave peligro de su perpetración. Las excepciones por motivos de sanidad o de grave riesgo son reguladas por la ley.

En la practica el habeas data en Perú funciona tanto como un instrumento protector de la privacidad pero tambien como una norma de acceso a la informacion publica para el ciudadano. Existen varios casos relativos a ambas instancias. EL habeas Data esta reglamentado procesalmente.

2.7 Paraguay

La Carta Magna de Paraguay contiene una serie de interesantes normas sobre libertad de expresión y derecho a la privacidad. La Constitución de Paraguay de 1992 regula el habeas data en el art. 135: *Toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos si fuesen erróneos o afectaran ilegítimamente sus derechos.*

2.8. Uruguay

En cuanto al Habeas Data, no existe en Uruguay previsión legal ni constitucional alguna que lo contemple. En un articulo publicado en REDI, titulado La protección jurídica de los "datos personales" y los servicios de información comercial y crediticia, Marcelo Bauzá Reilly da un panorama del habeas. Este autor sostiene que el *país no*

tiene ... normas de carácter especial sobre esta cuestión de los "datos personales" y su regulación jurídica, aunque existen síntomas que permiten deducir que las tendrá en fecha no lejana. Y si bien un régimen en forma necesita mayores previsiones, no hemos seguido hasta el momento, siquiera, la reciente tendencia latinoamericana de incluir artículos constitucionales contemplativos del instituto de habeas data, siendo el único país del Mercosur que no lo ha hecho. Exceptuando unas pocas previsiones sectoriales ... la situación es de vacío -o prácticamente tal- en cuanto a la existencia de un régimen específico que regule la apropiación y uso de los datos personales por parte de Estado y los particulares terceros.

2.9 Venezuela

La reforma de la Constitución en 1999 incluyo una cláusula contemplando el habeas data.

3.- RAZONES POR LAS CUALES ES NECESARIO UNA LEGISLACION GENERAL SOBRE PROTECCION DE DATOS EN LATINOAMERICA:

- Hemos repasado como la mayoría de los países en Latinoamérica han incorporado normas sobre Habeas Data en sus Constituciones y como algunos están incluyendo leyes de protección de datos personales.

- El Habeas data es una herramienta procesal que sirve solo cuando el daño ocurrió. Las leyes de protección de datos tienen un carácter preventivo, pues establecen normas para el manejo de los datos personales. Quienes tratan este tipo de información deben poner cierta diligencia en el manejo de los datos personales y privacidad de los individuos.

- El modelo europeo se ha extendido fuertemente fuera de los países miembros de la Unión Europea (Australia, Nueva Zelandia, Chile, Canadá, Hungría, Taiwan, Hong Kong, Japón, etc.). Además el modelo europeo tiene treinta años de experiencia.

- El análisis de la legislación latinoamericana es muy importante también como medio de estudiar la existencia de estándares relativos al derecho a la privacidad en Latinoamérica, con especial referencia al articulo 25 de la Directiva Europea de Protección de Datos que prohibe la transferencia de datos personales a países que no tengan un régimen adecuado de protección de privacidad. Si se siguen las pautas establecidas por la Unión Europea para analizar si un país posee legislación adecuada, podrá comprobarse que en Latinoamérica solo Chile cumple adecuadamente con los requisitos de la Directiva. Esto eventualmente podría producir un bloqueo en la transferencia internacional de datos de empresas latinoamericanas en Europa.

- Además el auge del comercio electrónico va a requerir un sistema uniforme de protección a la privacidad de modo que este no se transforme en un obstáculo para su desarrollo dentro de Latinoamérica.

- Elaborar el sistema uniforme en Latinoamérica evitaría el problema que afronto Europa en la ultima década relativo a la necesidad de armonizar sus leyes por los posibles obstáculos a las transferencia de datos personales.

- Por otra parte, elaborar un sistema uniforme de protección de datos en Latinoamérica parece mas viable a corto plazo que la alternativa de realizar un Acuerdo al nivel de la OMC sobre Estándares para el tratamiento de Información Personal.

- Por ultimo, es necesario la creación de Agencias de Protección de Datos a nivel latinoamericano para velar por el cumplimiento de las leyes de protección de datos.

4. PROPUESTAS DE REGLAMENTACION DEL HABEAS DATA EN LATINOAMERICA.

Como forma de superar el vacío existente en Latinoamérica en materia de protección de datos personales proponemos las siguientes medidas:

1) Crear leyes de protección de datos siguiendo el modelo europeo.

2) Como paso previo al dictado de la ley, implementar dentro del sector publico las Directrices de la Organización para la Cooperación y el Desarrollo Económico (con un simple decreto que liste en un anexo su contenido) y promover su adopción en el sector privado a través de uniones industriales y cámaras empresarias.

3) Promover un Convenio Latinoamericano al estilo del Convenio No. 108 del Consejo de Europa (podría realizarse a nivel del PSJCR o la OEA).

4) Promover la creación de organismos rápidos, flexibles y no burocráticos que tengan facultades sancionatorios y reglamentarias en materia de protección de datos de modo de evitar abusos del poder informático (estas conclusiones ya estaban presentes VI Congreso de Derecho e Informática de Uruguay y proponemos que se repitan ante la ausencia de recepción por parte de los gobiernos latinoamericanos).

5) Reglamentar el habeas data a nivel constitucional –en los países donde aun no ocurrió-, y a nivel procesal de modo que se establezca como una herramienta efectiva para el control de los datos personales, posibilitado el desarrollo pleno del individuo y su protección en la sociedad tecnológica.

NOTA FINAL: La recopilación de información sobre el Habeas Data en Latinoamérica forma parte de la tesis doctoral del autor. Se agradecerá la remisión de información actualizada sobre sus respectivos piases a pablopalazzi@ulpiano.com o pablopalazzi@yahoo.com. El lector podrá consultar un listado de las legislaciones y normas constitucionales sobre protección de datos en la siguiente dirección de Internet: http://ulpiano.com/Recursos_Privacy_Dataprotection.htm

La Firma Digital y la Autoridad Certificante en Uruguay

Dra. Esc. María José Viega Rodríguez (Uruguay)

1. INTRODUCCION

He presentado a este evento dos ponencias que tienen estrecha relación entre sí, por un lado el análisis de la prueba informática, un tema en el cual la seguridad es de suma importancia, como también lo es, en la contratación electrónica saber con certeza la identidad de la persona con la cual estamos contratando, que ésta existe realmente, que es capaz y que es el titular de los derechos de los cuales está disponiendo.

Como todos sabemos en EEUU se están realizado contrataciones en forma electrónica hace ya un buen tiempo, en forma exitosa entre los distintos Estados. Existen empresas privadas cuyo cometido es certificar la firma de los contratantes, a las cuales se les denomina "Autoridad Certificante", que veremos más adelante.

Pero resulta necesaria la existencia de una persona "...que fuera entendida en materia jurídica y capaz de redactar cláusulas de un contrato, que fuere imparcial en el negocio jurídico y que además de todo esto diera fe del acuerdo de voluntades y mantuviera bajo su custodia y responsabilidad (copia u original) el negocio jurídico."[1]

Y advierten que existe un profesional en el ámbito jurídico, que es el Notario u Escribano, en el marco del Notariado Latino, que se adapta a los requerimientos de la contratación electrónica. Es así como surgió el proyecto "Cybernotary", que concluyó con una ley en el Estado de la Florida que concretó el proyecto, creando un profesional del derecho (Abogado), que además tuviera conocimiento del sistema EDI, al cual se lo dotó de la potestad de certificación.

Por lo tanto, la función del escribano es de suma importancia en la contratación electrónica, y sin lugar a dudas va a estar determinando el éxito o fracaso de una negociación.

2. ELEMENTOS DE RELEVANCIA PARA LA CONTRATACION ELECTRONICA:

Cuando realizamos un contrato en forma electrónica es de fundamental importancia que la transferencia de información sea un sistema seguro, para lo cual es importante tener en cuenta los siguientes elementos:

a) Confidencialidad: la comunicación no debe estar expuesta a terceras personas, ni permitir que estas comprendan el mensaje que se está trasmitiendo.

b) Integridad de la transacción: es importante tener la certeza que el mensaje trasmitido y recibido por la otra parte esté completo y no halla sufrido modificación alguna.

c) Identificación de las partes: debemos tener seguridad de quien es la persona con la cual nos estamos comunicando.

d) Seguridad de la transacción: Toda comunicación debe estar firmada, de forma tal que el negocio tenga expresado el consentimiento de forma inequívoca.

---

[1] De la Fuente, Juan Angel. "La intervención notarial en la contratación electrónica". Libro de Ponencias del VI Congreso Iberoamericanode Derecho e Informática. Montevideo - Uruguay . 1998.

3. DIFERENTES TIPOS DE FIRMA.

a) *Firma ológrafa o tradicional:* cuando una persona "firma" un documento en papel está manifestando su voluntad y lo que hace es dibujar sobre él una serie de símbolos que lo identifican.

Pablo Palazzi[2] define la firma como *"el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad"*.

La firma en este caso cumple diversas funciones, lo cual dependerá de la naturaleza del documento:

- Establecer la autoría del propio texto.
- Aceptar las obligaciones que surgen de un texto.
- Adherir a lo expresado por otro.
- Determinar la presencia del mismo

Cuando un Escribano certifica una firma lo que está asegurando es que la persona que firma es quien dice ser, que lo hizo libre y conscientemente, que firmó dicho documento en un lugar y día determinado.

Dice Palazzi[3] que: *"Si se encuentra un medio que reemplace a la firma ológrafa en ambientes digitales, éste nuevo medio deberá cumplir con las funciones tradicionales de la firma. Estas son: (i) indicativa: informa acerca de la identidad de un autor; (ii) declarativa: se refiere al acuerdo respecto al contenido del acto; (iii) probatoria: permite vincular al autor con el signatario"*.

b) Firma electrónica: con relación a las diferentes técnicas utilizadas para firmar electrónicamente un documento, Guillermo Balay[4] describe las siguientes: "Una técnica disponible es el uso de una tableta sensible y un lápiz magnético conectados a un PC donde se registra la presión, velocidad y coordenadas donde el operador apoya el lápiz. Esos datos se combinan matemáticamente para formar la "firma electrónica" de la persona. Posteriormente, se puede comparar esa firma almacenada con otra para verificar si pertenecen a la misma persona.

Otra técnica de firma electrónica disponible en el mercado podría ser el registro de la huella digital y de ciertos factores biológicos de la piel que identifican unívocamente a la persona. El dispositivo consiste en un tablero donde la persona coloca su dedo. Allí se digitalizan la huella y los parámetros biológicos del dedo de la persona, de tal forma que es imposible reproducirlos salvo que se obligue a la persona a colocar su dedo en el dispositivo".

c) Firma digital: en sí misma es un dato (secuencia de bits) y el peligro radica en que una vez divulgado, cualquiera puede utilizarlo y hacerse pasar por su titular.

Para que esto no suceda, en la firma digital se utiliza lo que se denomina "criptografía de clave pública".

Vayamos por partes. La criptografía es la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Es una rama de las matemáticas que procura hacer incomprensibles los mensajes, para que no puedan ser leídos por terceros, y luego tornarlos a su estado natural.

---

[2] Palazzi, Pablo Andrés. "Firma digital y comercio electrónico en Internet". VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, 1998.

[3] Idem cita anterior.

[4] Balay, Guillermo. "Enfoque informático del Decreto N° 65/998". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

Existen dos tipos de criptografía:

* de clave secreta: tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave. Es una forma conocida también como simétrica. El peligro que acarrea es que normalmente las personas no se conocen personalmente, por lo tanto el canal para el envío de la clave debe ser un canal seguro.

* de clave pública: es un sistema asimétrico, y fue creado en Estados Unidos en el año 1976. No es necesario en esta caso un canal seguro porque cada persona dispone de dos claves, un pública (conocida por todos) y otra privada (conocida únicamente por el titular). Para encriptar el mensaje el remitente utiliza la clave pública del destinatario, de tal manera que solo el destinatario pueda descencriptarlo con su clave privada. Con relación a la seguridad de este sistema el P/S Guillermo Balay[5] dice que: "Ambas claves de un mismo usuario están relacionadas matemáticamente, pero es casi imposible calcular la clave privada a partir de la pública, aún conociendo el algoritmo empleado para construirlas".

Este es el sistema utilizado en la firma digital, el emisor cifra el mensaje con la clave pública del receptor, y firma el mensaje aplicando su clave privada; el receptor del mensaje utiliza su clave privada para descifrar el mensaje y la clave pública del emisor para verificar la firma digital.

4. FIRMA ELECTRONICA Y DIGITAL EN NUESTRO DERECHO.

Nuestro derecho incorporó la firma digital para el Procedimiento Administrativo en la Administración Central por Ley 16.736 en el artículo 695, el cual equipara los medios informáticos a los convencionales, reconoce su validez jurídica y les otorga el mismo valor probatorio. El inciso final de este artículo consagra expresamente la firma electrónica digital.

El **Decreto 65/998** reglamentario de la ley 16.736, en su artículo 1 inciso final establece: "*Cuando la substanciación de las actuaciones administrativas se realice por medios informáticos, las firmas autógrafas que la misma requiera podrán ser sustituidas por contraseñas o signos informáticos adecuados*".

Este artículo es de una gran amplitud, ya que no establece que tipo de firma sustituirá a la firma autógrafa. Sin embargo en los artículos 18 y 19 definirá la firma electrónica y digital, diferenciándolas.

El artículo 18 define la **firma electrónica**, y dice que es "*el resultado de obtener por medio de mecanismos o dispositivos un patrón que se asocie biunívocamente a un individuo y a su voluntad de firmar.*"

Comentando este artículo dice el Dr. Ruben Correa Freitas[6] que "*Esto es lo que comúnmente en informática se conoce como el "password" o contraseña, que es la clave informática que tiene una persona y que solamente ella la puede usar*".

Y el artículo 19 define la firma digital como: "*un patrón creado mediante criptografía, debiendo utilizarse sistemas critográficos "de clave pública" o "asimétricos", o los que determine la evolución de la tecnología*". Me parece de suma importancia que el artículo deja una puerta abierta a los avances tecnológicos.

---

[5] Idem cita anterior.

[6] Correa Freitas, Ruben. "Principios del Procedimiento Administratico Electrónico. Decreto del Pode5r Ejecutivo N° 65/998 de 10/III/98". Procedimiento Administrativo Electrónico. Publicación de la Oficina Nacional del Servicio Civil. Presidencia de la República.

5. AUTORIDAD CERTIFICANTE.

Es un tercero imparcial, confiable para ambas partes y para la sociedad toda, dotado de poderes de certificación. Las autoridades certificantes están autorizadas a emitir certificados digitales, que detallaremos más adelante.

Las funciones de la autoridad certificante son las siguientes:

a) publicar las claves públicas,

b) realizar la identificación física antes de entregar las claves y posteriormente controlar si la clave pública pertenece a la persona que dice ser su titular,

c) certificar el procedimiento de identificación,

d) publicar siempre que se dé una situación de suspensión, revocación, extinción o modificación de la clave pública.

6. AUTORIDAD CERTIFICANTE EN URUGUAY.

El art. 2 de la Ley 16736 de 1995 establece: "*La Administración Nacional de Correos tendrá a su cargo la prestación de servicios postales, esto es la admisión, transporte, o distribución y entrega de envíos de correspondencia, giros postales, y productos postales en general*".

Se entiende la correspondencia electrónica como un tipo especial de correspondencia, ya que la diferencia está en el soporte que contiene la información y en la forma de transferirla, por lo que la certificación está dentro de sus cometidos.

A través de la "Recomendación de la Comisión Nacional de Informática de fecha 25 de setiembre de 1998": se autoriza a la Administración Nacional de Correos a prestar servicios de Autoridad de Certificación en todo el país.

Establece la Administración Nacional de Correos[7]: "*La importancia de una Autoridad de Certificación en el contexto de las comunicaciones globales está dada no solamente por su confidencialidad y respeto nacional, sino también por su reconocimiento internacional. A este respecto corresponde destacar que la Administración Nacional de Correos integra la Unión Postal Universal (UPU) y la Unión Postal para las Américas, España y Portugal (UPAEP), organismos internacionales que tienden al incremento mundial de las comunicaciones postales. Los correos más importantes del mundo se han posicionado ya como Autoridad de Certificación Nacional en sus respectivos países, lo que constituye una verdadera Red Internacional con sólido respaldo y trayectoria.*"

7. CERTIFICADOS EMITIDOS POR EL CORREO:

1. Certificados Personales (Identificación segura): para personas que desean realizar transacciones electrónicas a título personal.
   Requisitos: 18 años de edad y documento de identidad o pasaporte.

2. Certificados Empresa (Empresa segura): son emitidos para personas que van a representar a una Empresa.
   Requisitos: persona mayor de 18 años, se verifica la identidad de la persona y de la empresa y documentación que habilite a actuar en representación de la misma.

[7] Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy

3. Certificados para servidores (Sitio seguro): "generalmente servidores de publicación de páginas Web. Estos certificados permiten la habilitación del protocolo SSL (https://) para el acceso seguro a la información publicada, dando garantías a los clientes de estar accediendo al servidor correcto. En este caso se verifica con la autoridad responsable correspondiente que el nombre de dominio solicitado corresponda a la empresa solicitante y se verifica la identidad del servidor."[8]

Las claves y el certificado se entrega al titular, no quedando copia de las claves en los servicios de Certificación de la A.N.C. El medio en que se entrega puede ser un disquete o una tarjeta Smart Card.

8. CONCLUSIONES.

En un trabajo realizado por la Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino *"El notario y las transacciones jurídicas electrónicas"*[9] al referirse a la autoridad certificante manifiesta: *"Esta infraestructura de certificación crea nuevas posibilidades para el notariado, que podrá proponerse como garante de la procedencia de actos públicos de un estado a otro, brindando a la función notarial la plenitud y prestigio que ha gozado en la era papel"*.

En nuestro país, si bien se consagró a la Administración Nacional de Correos como la autoridad certificante, la misma se limita a emitir los certificados que hemos vistos, no estamos ante el tercero imparcial que redactara el negocio, que recabara los consentimientos, que tuviera conocimientos jurídicos para asesorar a las partes y que además certificara su firma. Por lo tanto, elaborar un proyecto de ley sobre firma digital se impone, la calidad certificadora es nuestra tarea por naturaleza y debe seguir siéndolo en el mundo digital.

Esto nos demuestra, que lejos de las visiones apocalípticas del notariado para este siglo, como consecuencia de los adelantos tecnológicos, estamos preparados para continuar desarrollando nuestra función, que materialmente tendrá sin lugar a dudas cambios de importancia, pero siempre basado en los principios que nos rigen desde los orígenes, dando transparencia y certeza al negocio jurídico

BIBLIOGRAFIA

1. Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy

2. Correa Freitas, Ruben. "Principios del Procedimiento Administratico Electrónico. Decreto del Pode5r Ejecutivo N° 65/998 de 10/III/98". Procedimiento Administrativo Electrónico. Publicación de la Oficina Nacional del Servicio Civil. Presidencia de la República.

3. De la Fuente, Juan Angel. "La intervención notarial en la contratación electrónica". Libro de Ponencias del VI Congreso Iberoamericanode Derecho e Informática. Montevideo - Uruguay . 1998.

4. Palazzi, Pablo Andrés. "Firma digital y comercio electrónico en Internet". VI Congreso Iberoamericano de Derecho e Informática. Libro de Ponencias. Montevideo – Uruguay, 1998.

5. Balay, Guillermo. "Enfoque informático del Decreto N° 65/998". Procedimiento administrativo electrónico. Presidencia de la República. Oficina Nacional del Servicio Civil. 1998.

6. Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino "El notario y las transacciones jurídicas electrónicas", publicada www.colegio-escribanos.org.ar/ediciones.htm

[8] Página de la Administración Nacional de Correo publicada en Internet: www.correo.com.uy

[9] Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino "El notario y las transacciones jurídicas electrónicas", publicada www.colegio-escribanos.org.ar/ediciones.htm

RESUMEN

Este trabajo pretende dar una conceptualización del tema firma digital, así como la importancia de la misma en la contratación electrónica.

Además, hemos analizado las normas que regulan la temática en el derecho uruguayo en el ámbito administrativo, así como también la designación de la Administración Nacional de Correos como Autoridad Certificante.

También ha sido nuestro objetivo destacar la importancia de la existencia del notario o escribano, dejando de lado las visiones apocalípticas acerca de nuestra profesión como consecuencia del avance de la tecnología.

Nombre: **Dra. Esc. María José Viega Rodríguez**
Nacionalidad: **Uruguaya**
Dirección: **Calle 25 de Mayo 477 Esc. 46 Montevideo Uruguay.**
Teléfono: **915 41 90 – 099 19 34 78**
Fax: **915 41 90**
Email: **mjviega@adinet.com.uy**

CURRICULUM:

- Doctora en Derecho y Ciencias Sociales.
- Escribana Pública.
- Integrante de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay.
- Aspirante a la materia Informática Jurídica en la Universidad de la República.

El Comercio Electrónico: ¿Hacia una Nueva Revolución Económica y Jurídica?

Pedro Juez Martel (España)
(Vicedecano Facultad de Derecho UNED)

1. INTRODUCCION

Sin ningún lugar a dudas Internet es una de las mayores revoluciones que han existido en este siglo. Las perspectivas que existen para el comercio y la economía son todavía insospechadas. En esta ponencia se pretende responder a las siguientes preguntas:

1. ¿Qué se entiende por comercio electrónico?
2. ¿Qué evolución ha existido y cuál es su previsión?
3. ¿Cuáles son sus principales problemas y cómo se pueden resolver? .

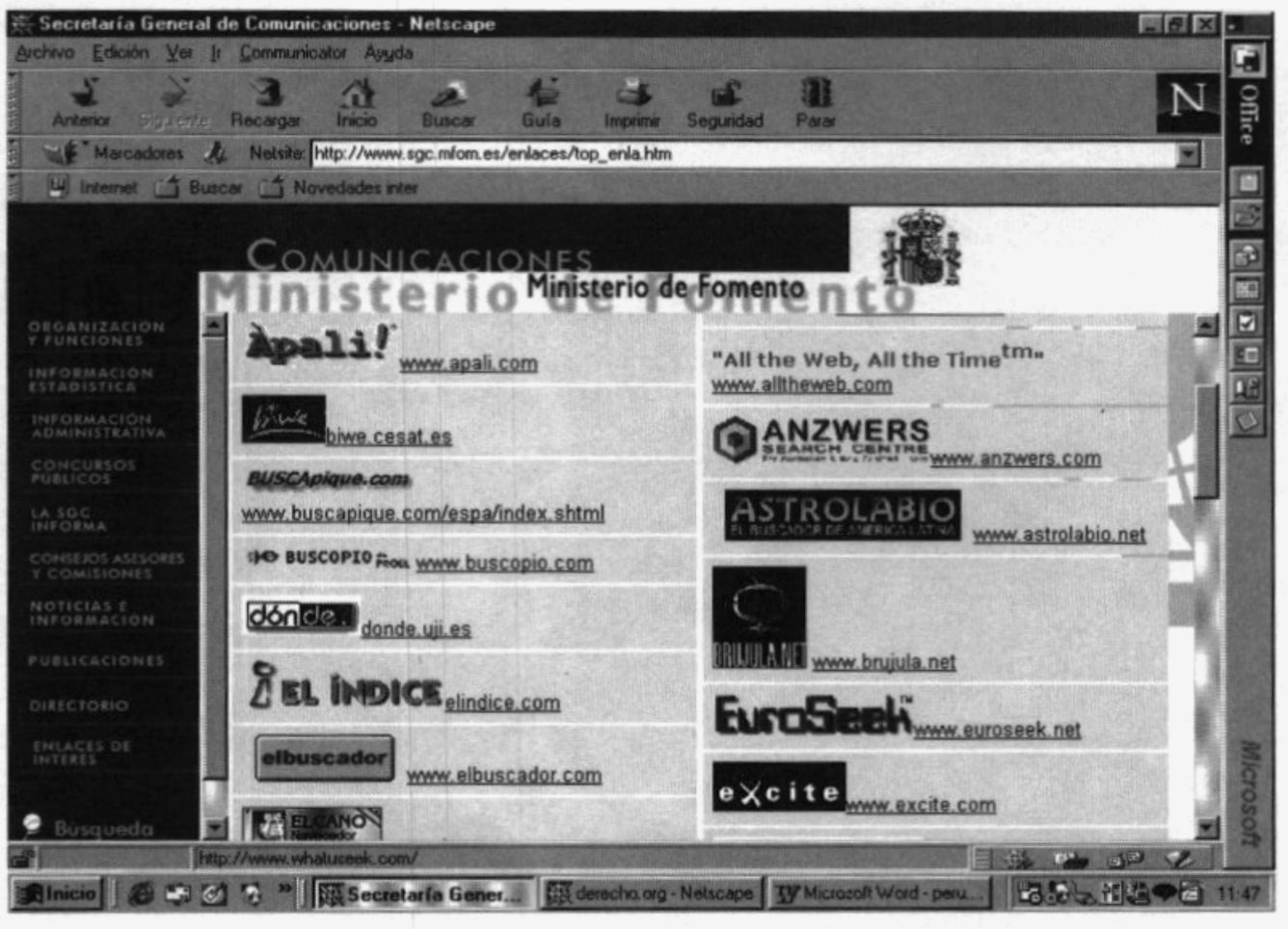
2. CONCEPTO DE COMERCIO ELECTRONICO

Respecto a la primera pregunta, el comercio electrónico se puede entender como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet.

El concepto de comercio electrónico no sólo incluye así a la compra y venta electrónica de bienes, información o servicios, sino también al uso de la Red para actividades anteriores o posteriores a la venta, como son:

La publicidad: El acceso de un número cada vez mayor de usuarios ha hecho de Internet un medio muy valorado en cuanto a la publicidad. El número de empresas que se anuncian en la red de acuerdo con datos proporcionados por Adrelevance la publicidad en la red ha aumentado un 58 por ciento en 1999. Se prevé que para el año 2003 el medio publicitario moverá 15.000 millones de dólares, es decir, unos 225 billones de pesetas. Las dos terceras partes de este tipo de publicidad es realizado por empresas tecnológicas. La subida en los mercados bursátiles de las empresas relacionadas con Internet ha sido imparable en los últimos meses.

La búsqueda de información sobre productos, proveedores, etc. : el número de empresas se ha multiplicado por diez en los últimos años. Ahora más que nunca Internet se ha convertido en una plataforma con alcance a nivel mundial. La creación de más y mejores buscadores ante la avalancha de información en la red debe ser uno de los principales objetivos de Internet.



La negociación entre comprador y vendedor sobre precio, condiciones de entrega, etc.: **Existen numerosas páginas dedicadas a subastas de todo tipo de bienes, que van desde bienes inmobiliarios, viajes, o todo tipo de objetos.**

La atención al cliente antes y después de la venta: **Empresas como Hewlett-Packard realizan ya a través de la red buena parte de su servicio de atención al cliente.**

La colaboración entre empresas con negocios comunes **(a largo plazo o sólo de forma coyuntural): Es el denominado comercio electrónico B2B, de un desarrollo cada vez mayor.**

En el comercio electrónico participan como actores principales las empresas, los consumidores y las administraciones públicas. Se distinguen normalmente tres tipos básicos de comercio electrónico

- Entre empresas denominado también B2B (Business to Business)
- Entre empresa y consumidor o B2C (business to consumers)
- Entre empresa y administración o B2A (business to administrations)

Las empresas son las que ofrecen los servicios, los consumidores los que los adquieren, y la Administración regula, fomenta, y promueve. Asimismo la Administración puede emplearla también para obtener servicios, información, o convocar concursos públicos).

2. EVOLUCION Y TENDENCIA DE INTERNET

En primer lugar parece claro señalar que esta evolución está muy ligada al número de usuarios de internet. Aunque las opiniones son dispares, todos las consultoras coinciden en un crecimiento exponencial de los datos.

El desarrollo no es igual en todos los países. El país con mayor número de usuarios es EEUU, donde un informe de la consultora Strategis Group ha indicado que el número de usuarios ha superado ya los 100 millones de personas, es decir el 50 % de la población adulta. Hace sólo un año el número de usuarios era igual a 68 millones.

En el caso europeo, según un estudio de la consultora Forrester Research, sólo el 18 por ciento de los hogares europeos tienen acceso a Internet y menos del 10 por ciento compran a través de la red. Las dos terceras partes dijeron que preferían comprar en almacenes. De Europa el país con mayor número de usuarios es Francia donde la penetración del servicio de Minitel ha hecho que los franceses tengan una mayor confianza en el sistema. A este respecto un estudio del Grupo Benchmark ha señalado que las ventas a consumidores han pasado de 400 millones de Francos en 1998 a 1,3 billones en 1999. En España, según la última encuesta publicada por el Estudio General de Medios (EGM) el número de internautas españoles asciende a 2.747.000, el 8% de la población española. El estudio, realizado entre los meses de febrero y marzo de 1999, resalta el escaso incremento del número de personas con acceso a Internet, pese a que la población de estudio (todos los españoles mayores de 14 años) ha aumentado considerablemente. En cuanto al número de personas que se han conectado a la Red en el último mes, esta cifra sobrepasa por primera vez los dos millones, colocándose en 2.017.000 personas, frente al 1.733.000 de la oleada anterior. El 5´8% de la población de nuestro país se declara pues internauta más o menos habitual. Aunque el número de personas conectadas a la Red ha aumentado en un 0'9%, la cifra sigue siendo baja, tendencia acusada en el mercado español tras la subida de las tarifas telefónicas del pasado mes de agosto. Desde el verano de 1998 sólo se han detectado 500.000 internautas más en España, mientras que en las oleadas anteriores los crecimientos eran bastante mayores.

En otros continentes como Latinoamérica el despegue parece más lento. Actualmente, según la consultora norteamericana, Jupiter Communications existen unos 9 millones de usuarios. Esta cifra se espera que se incremente en un 50 por ciento hasta el año 2003 donde habrá unos 38 millones de personas en la red. El número de usuarios seguirá siendo relativamente baja, alrededor de un 6,8 por ciento de la población, y el mayor número de usuarios se concentrará en Brasil, Argentina, y México.

Respecto a las previsiones sobre la evolución del comercio electrónico en los próximos años (e incluso las estimaciones de su volumen actual) son también bastante dispares.

Según la OCDE, el volumen global del comercio electrónico ha pasado de prácticamente cero en 1995 a unos 25.000 millones de dólares en 1997. Las estimaciones superan los 300.000 millones de dólares para los años 2001-2002 y el billón de dólares hacia el 2003-2005. De estas cifras, el comercio entre empresas representa en torno al 80% del total. Según el mismo informe, Estados Unidos representaría el 80% del comercio electrónico mundial.

En el caso de Estados Unidos en sólo cuatro años, Internet se ha convertido en uno de los principales motores de la economía estadounidense. Sólo el pasado año la industria cibernética produjo 47 billones de pesetas por la venta electrónica y el comercio a través de la Red.

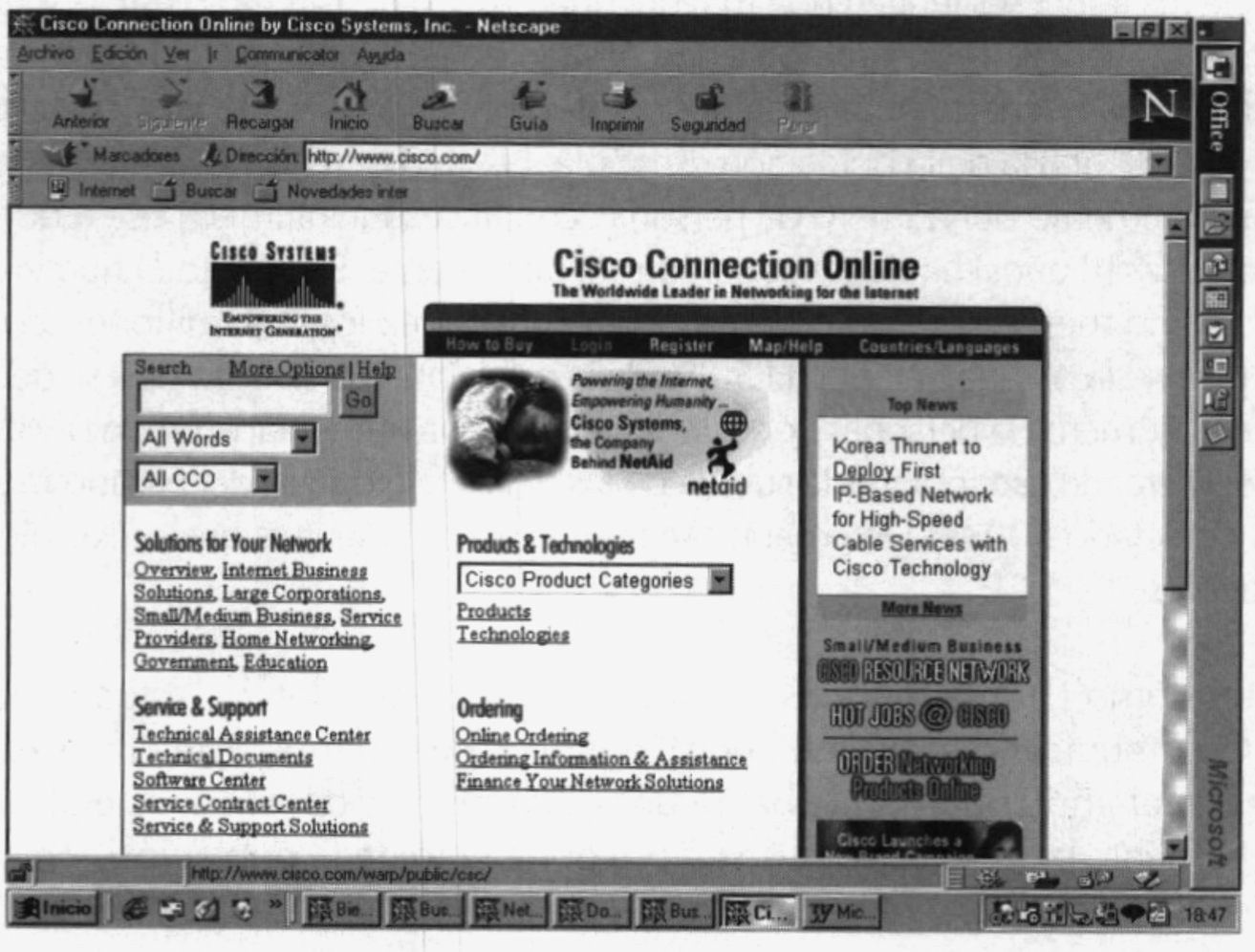
A Internet sólo le ha costado 48 meses lograr casi los mismos ingresos que la todopoderosa industria del automóvil en EEUU, que mueve unos 55 billones de pesetas anuales. Ni siquiera la industria de las telecomunicaciones puede superar al auge de la Red, sector que además emplea en estos momentos a 1'2 millones de personas en Estados Unidos, y que se incrementa a una media de un 174% anual.

La infraestructura, la construcción de los portales, el diseño de las páginas y los avances tecnológicos, que han hecho posible el rápido acceso de los internautas a la Red, fueron los apartados del sector que generaron más ingresos, con 17 billones de pesetas en 1998. El comercio fue el sector que empleó más personas, con unos 482.000 trabajadores en las más de 11.000 firmas que venden productos en el Web.

Dësde 1994 a 1998, la economía cibernética ha crecido una media de un 174 % cada año y ha superado todas las previsiones de crecimiento. Internet dobla sus ingresos cada 9 meses y en la actualidad emplea a 1,2 millones de personas. En este apartado de nuevo el Web empequeñece a otras industrias más conocidas e históricas como Wall Street que da empleo a unas 125.000 personas.

En el comercio entre empresas las previsiones según la empresa consultora Gartner es que llegarán a los 29 trillones de dólares en el año 2.004. Actualmente se encuentran en 145 billones de dólares.Respecto al comercio entre empresas europeo la consultora Gartner estima que se incrementará de 31,8 billones de dólares en 1999 a 2,34 trillones en el año 2004

Cisco Systems empresa norteamericana dedicada al suministro de material informático, que concentra especialmente sus esfuerzos en Internet es desde finales del mes de marzo la empresa con mayor capitalización bursátil del mundo.



Lo cierto es que las previsiones, aunque dispares, coinciden en señalar la gran evolución que el comercio electrónico está teniendo. Este auge se debe a que el comercio electrónico tiene una serie importante de ventajas como son:

- Reducir las barreras de acceso a los mercados actuales, en especial para pequeñas empresas abriendo oportunidades de explotar mercados nuevos. El mercado se ve ampliado a todo aquellos usuarios que a nivel mundial dispongan de Internet.

- Para el consumidor, ampliar su capacidad de acceder a prácticamente cualquier producto a nivel mundial, permitiendole la comparación de ofertas para un mismo producto.

- Reducir o incluso eliminar por completo los intermediarios, por ejemplo en la venta de productos en soporte electrónico (textos, imágenes, vídeos, música, programas, etc.) que se pagan y entregan directamente a través de la red.

No obstante, ¿Cuáles son los principales problemas para su desarrollo?

Los problemas para su desarrollo tienen dos claras vertientes: legal y tecnológica.

4. PROBLEMATICA LEGAL DEL COMERCIO ELECTRONICO

- **Legal:** Los problemas legales se pueden resumir en los siguientes aspectos:

1. Producción de contratos "sin papel" con escasa validez jurídica.

2. Generación de fraudes fiscales al existir transacciones no controladas por el fisco.

3. Quebrantamientos de la protección de los derechos de propiedad intelectual.

4. Indefensión de los consumidores ante publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales

5. Falta de tipicidad penal y de policía especializada en el control de conductas antijurídicas.

6. Falta de seguridad y confianza al suministrar los datos de la tarjeta de crédito, y en general sobre los medios de pago. Una reciente encuesta realizada en EEUU por el Instituto de Tecnología de Georgia sobre una muestra de más de 12.000 usuarios de la red a nivel mundial, constataba. que ante la pregunta acerca de la seguridad de los medios de pago más del 60 % consideraba que no existía o era escasa.

7. Preocupaciones sobre problemas acerca de la fiabilidad del vendedor, la devolución del producto, la utilización de datos personales para el envío de publicidad no deseada, o la cesión de éstos a otras empresas.

Soluciones jurídicas

De este modo para que el comercio electrónico funcione adecuadamente será necesario tener un entorno legal que resuelva los aspectos de seguridad y privacidad, validez legal de los documentos comerciales en formato electrónico, fiscalidad, derechos de propiedad intelectual, etc., y que además la regulación esté globalizada a nivel mundial.

Deben así existir un conjunto básico de estándares implementados en herramientas de comercio electrónico integradas, abiertas e interoperables. Aunque varias organizaciones han propuesto arquitecturas o modelos generales de comercio electrónico que tratan de conseguir estos objetivos de integración y compatibilidad, muchas de estas propuestas están todavía en evolución, y no está definida la aceptación que tendrá cada una en el mercado.

Respecto a la seguridad se han arbitrado distintas posibles soluciones técnicas como son las técnicas criptográficas, en particular los métodos de cifrado simétrico (usan una misma clave secreta para cifrar y descifrar) o asimétrico (cada usuario tiene una pareja de claves, una pública y otra privada, con la propiedad de que lo que se cifra con una de las claves sólo se puede descifrar con la otra).

Este último sistema es por el que se parecen inclinar más las autoridades. Con arreglo a él cada usuario tiene parejas de claves (una pública y otra privada) con la propiedad de que lo que se cifra con una cualquiera de las claves de una pareja sólo se puede descifrar con la otra clave de la pareja. Cada interlocutor hace pública una de sus claves (la clave pública) y mantiene en secreto la otra (su clave privada). La clave privada (o las claves privadas si el usuario utiliza varias parejas de claves para diferentes propósitos) puede guardarse en el ordenador del usuario o en una tarjeta inteligente.

Por la propiedad de las parejas de claves citada antes, para enviar un mensaje de forma confidencial a un destinatario basta cifrarlo con la clave pública de ese destinatario. Así sólo el podrá descifrarlo mediante la clave privada que mantiene en secreto. No es necesario que el remitente y el destinatario intercambien previamente ninguna clave secreta. El remitente sólo necesita averiguar la clave pública del destinatario. Para evitar posibles suplantaciones de identidad, es necesario contar con una tercera parte fiable que acredite de forma fehaciente cuál es la clave pública de cada persona o entidad. Esta es la función básica de las autoridades de certificación.

El procedimiento de autenticación de la firma digital de un mensaje o contrato de compraventa mediante este sistema consiste en colocar la firma en un "resumen" (o hash en inglés) del mensaje, cifrándola con la clave privada del remitente. Este "resumen cifrado" en el que iría la firma se colocaría al final del mensaje. A continuación, el mensaje más la firma (el resumen cifrado) se envían como antes cifrados con la clave pública del destinatario. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a un resumen diferente. (Nótese que la firma digital de un usuario no es siempre la misma secuencia de bits, sino que depende del mensaje firmado.)

Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma. Para ello, hace dos operaciones: por un lado averigua la clave pública del remitente y descifra con ella el resumen (la firma) que cifró el remitente. Por otro lado, el destinatario repite el procedimiento que usó el remitente. Si los dos resúmenes (el del remitente descifrado y el envíado ahora por el destinatario) coinciden la firma se considera válida y el destinatario puede estar seguro de la integridad del mensaje: si el mensaje hubiera sido alterado a su paso por la red, el resumen calculado por el destinatario no coincidiría con el original calculado por el remitente.

Además, el hecho de que el resumen original se ha descifrado con la clave pública del remitente prueba que sólo él pudo cifrarlo con su clave privada. Así el destinatario está seguro de la procedencia del mensaje (autenticación del origen) y, llegado el caso, el remitente no podría negar haberlo enviado (no repudio) ya que sólo él conoce su clave secreta.

Los inconvenientes de este sistema son la lentitud de los algoritmos de clave asimétrica (típicamente varia veces más lentos que los de clave simétrica) y la necesidad de las autoridades de certificación digital. Un certificado digital emitido por una de estas autoridades contendría la identidad de un usuario, su clave pública y otros datos adicionales (por ejemplo, el periodo de validez del certificado), todo ello firmado digitalmente con la clave privada de la autoridad de certificación, con el fin de que el certificado no se pueda falsificar. Pueden existir varios tipos de certificados, válidos para diferentes usos, según la información y garantías que la autoridad de certificación (directamente o a través de una autoridad de registro) pide al usuario antes de emitir el certificado.

La Comisión Europea publicó en octubre de 1997 una comunicación sobre un marco común europeo para firma digital y cifrado y más recientemente, en mayo de 1998, una propuesta de directiva sobre un marco común

para firma electrónica. Esta propuesta establece requisitos mínimos para el reconocimiento legal de la firma digital en la Unión Europea, así como para el funcionamiento de las autoridades de certificación, incluyendo sus posibles responsabilidades.

Según la directiva, la firma digital es asimilable a la firma convencional y, llegado el caso, tiene valor probatorio en un juicio, supuesto que la firma digital está basada en un certificado emitido por un proveedor de servicios de certificación que cumple con los requisitos establecidos en la directiva.

En cuanto a estos proveedores (es decir, las autoridades de certificación) la directiva establece el principio de libertad de prestación de servicios de certificación sin autorización previa y sin restricciones entre países de la Unión Europea. Cada país deberá garantizar que los proveedores cumplen requisitos suficientes en cuanto a capacidad técnica, fiabilidad de los sistemas utilizados, suficientes recursos financieros, conservación de los datos relativos a los certificados emitidos y publicación de prácticas aplicadas por el proveedor, condiciones de los contratos, obligaciones de responsabilidad del proveedor y procedimientos de reclamación.

La directiva establece también el contenido mínimo de los certificados:

Identificación de la autoridad de certificación

Nombre del titular del certificado

Clave pública del titular

Periodo de validez del certificado

Algoritmos utilizables

Identificador único del certificado

Limitaciones de uso del certificado

Limitaciones de responsabilidad de la autoridad certificadora

Firma digital de la autoridad

La autoridad de certificación responde de la exactitud de la información del certificado (excepto que se indique lo contrario en el penúltimo punto de los citados en la lista anterior), de la correspondencia entre la clave pública que figura en el certificado y la clave privada del titular y, en general, del cumplimiento de los requisitos de funcionamiento mencionados anteriormente. La directiva permite introducir limitaciones de responsabilidad de las autoridades de certificación, por ejemplo limitándola a una cantidad máxima prefijada.

En cuanto a los aspectos de protección de datos personales, la directiva establece la posibilidad de solicitar certificados con un seudónimo, la prohibición de utilizar los datos del solicitante para otro fin que no sea el de la emisión del certificado y, en general, el cumplimientos de las normas derivadas de las directivas sobre protección de datos de 1995 y 1997. Se ha anunciado que el consejo de ministros aprobó en Diciembre de 1999 un Real Decreto sobre firma digital. Éste sigue prácticamente las directrices que se marcan en la Directiva comunitaria.

En lo que se refiere a comercio electrónico el Ministerio de Fomento español está preparando un anteproyecto cuyas directrices generales son las siguientes:

- Régimen de libre competencia y de libre prestación de servicios.

- Restricciones al libre establecimiento y prestación de servicios. Se establecen restricciones cuando se atente contra la seguridad nacional, los derechos fundamentales, y el orden público.

- Se establece un Registro de Prestadores de Servicios de la Sociedad de la Información. Este Registro se constituye a efectos de mera constancia, inspección y control. Lo único que se exige a los operadores es que soliciten su inscripción antes de iniciar su actividad.

- Se establece unos mínimos de información que los oferentes de servicios de comercio electrónico deberán suministrar a los usuarios.

- Establecimiento de regímenes de responsabilidad para operadores de redes y proveedores de acceso.

- Definición de unos parámetros de protección de los consumidores y usuarios respecto de la comunicación comercial por correo electrónico no solicitada.

- Contratos celebrados por vía electrónica: se parte del principio de validez de estos contratos y se indica la información que debe suministrar el oferente de los servicios a los consumidores y usuarios. Se regula, igualmente, el régimen a seguir para la formulación de las peticiones y el de prueba de las obligaciones.

- Lugar de celebración del contrato y jurisdicción competente: el contrato electrónico se presume celebrado en el lugar desde el que el destinatario del servicio efectúe su pedido, salvo que ninguna de las partes contratantes sea consumidor o usuario y ambas pacten lo contrario. El lugar de celebración del contrato así determinado, servirá para interpretarlo conforme a los usos y costumbres para determinar, en su caso, la exigencia de requisitos especiales para su formalización y la jurisdicción competente para conocer de su impugnación o exigir su cumplimiento.

- Arbitraje telemático: se prevé la posibilidad de la formalización telemática del arbitraje, siempre que se respete lo establecido en la actual normativa, particularmente en la contenida en la Ley de Arbitraje y en el Real Decreto Ley sobre Firma Electrónica. En los contratos celebrados por vía electrónica se podrá incorporar, con cláusula adicional, un convenio de sumisión a arbitraje de las partes para resolver las controversias que surjan entre ellas y su interpretación y ejecución.

- Vigilancia, control y régimen de infracciones y sanciones: para asegurar el cumplimiento de lo previsto en la norma que se proyecta, se establece un régimen de vigilancia y control, en beneficio de los consumidores y usuarios, atribuyendo a la Secretaría General de Comunicaciones la competencia de garantizar su eficacia y permitiendo ésta, en su caso, la adopción de las oportunas medidas cautelares, sin perjuicio de la eventual actuación de la Administración de Justicia.

OTRAS SOLUCIONES DE AMBITO EMPRESARIAL

En cualquier caso la solución y el desarrollo del comercio electrónico pasa por la creación de centros de investigación, y organismos de normalización, que con la ayuda de los diferentes Estados permitiesen crear un entorno de comercio electrónico accesible, seguro y fácil de usar , que genere confianza entre los usuarios, en particular entre los ciudadanos y las empresas pequeñas. La solución de los problemas legales y técnicos cambiará con toda probabilidad las relaciones comerciales que se han dado hasta la actualidad, abriendo a consumidores y empresas las puertas de un mercado de dimensiones mundiales.

En el caso español, con el fin de concienciar y fomentar la utilización del comercio electrónico se han creado distintas asociaciones una de ellas es la Asociación Española de Comercio Electrónico.(AECE). Es es una agrupación de empresas españolas que procuran unificar sus esfuerzos con el fin de obtener un comercio electrónico más fiable y seguro.Esta asociación nació en mayo de 1998 gracias al impulso de la Asociación Española de Marketing Directo (AEMD), que actuamente se denomina Federación de Comercio Electrónico y Marketing DirectoFECEMD). En diciembre de 1998, AECE incluía mas de 50 miembros.

AECE pretende hacer más flexible la legislación existente en materia de protección de datos personales y es partidaria de la autorregulación del sector de comercio electrónico. Una de las iniciativas destacables de AECE en esta línea es la elaboración de un código ético sobre el tratamiento de datos personales de consumidores obtenidos a través de Internet. Este código, que según AECE es pionero en Europa y será adoptado en otros países, se ha elaborado con la participación de la Agencia de Protección de Datos (APD), Asociación de Autocontrol de la Publicidad (AAP), Confederación de Consumidores y Usuarios (CECU), Organización de Consumidores y Usuarios (OCU) y Unión de Consumidores de España (UCE)

En esencia, el código propuesto se basa en el principio de permitir el uso de los datos siempre que los gconsumidores estén informados de los fines para los que una determinada empresa se propone utilizarlos (por ejemplo, para enviar información de otros productos, para ceder los datos a un tercero, etc.) y que se ofrezca al consumidor la posibilidad de restringir o prohibir dicho uso. AECE defiende por tanto el principio de uso de los datos en ausencia de negación expresa, frente al principio, más restrictivo, de usar los datos sólo cuando hay consentimiento expreso.

En 1998 entró en vigor la directiva europea sobre protección de datos y se abrió un proceso de revisión de la legislación española aplicable a este tema (la LORTAD). AECE, como se ha dicho, defiende la flexibilización de las limitaciones legales impuestas al uso de datos personales.

4. PROBLEMAS TECNOLOGICOS Y SUS SOLUCIONES

Junto con el problema legal, existen hoy en día otro tipos de problemas que están más relacionados con los aspectos tecnológicos y empresariales. Entre ellos podemos citar los siguientes:

1. Dificultad de encontrar información en internet, comparar ofertas y evaluar la fiabilidad del vendedor: Se debe decir a este respecto que faltan buscadores en la red, que permitan al usuario la comparación.

2. La congestión de Internet y la falta de accesos de usuario de suficiente capacidad: Mientras que en EEUU. Está generalizada la fibra óptica, esto no sucede en el caso español, donde la mayor parte de las conexiones continúan siendo por la vía telefónica. Esta es también una de las razones del desfase entre EEUU. y el resto de los países. Comunicaciones mucho más baratas y mejores medios, hacen muy difícil la igualdad a corto plazo

3. Concectando con el punto anterior está la lentitud en la transmisión de datos, video e imágenes a través de las convencionales líneas telefónicas. En este sentido, la queja más repetida de los usuarios es la del tiempo de espera al cargar las páginas Web.

En cualquier caso, aunque las características de seguridad de las redes y sistemas de comercio electrónico son, obviamente muy importantes, el hecho de que los usuarios consideren el comercio electrónico como suficientemente seguro depende menos de los detalles técnicos, y más de otras cuestiones como la confianza que inspiren las empresas vendedoras, financieras, etc.; la existencia y difusión de normas que, por ejemplo, limiten la responsabilidad del usuario en caso de uso indebido de una tarjeta de crédito y que garanticen su derecho a devolver un producto comprado electrónicamente; la creación de códigos éticos de comportamiento de las empresas y de procedimientos efectivos de solución de conflictos; etc.

CONCLUSIONES

La seguridad en las transacciones es el aspecto que más frena al consumidor. Internet está avanzando exponencialmente, y lo continuará haciendo en los próximos años. Sin embargo, el crecimiento europeo estará muy

condicionado por el desarrollo legal y de seguridad en la red. Prioritarias serán también las soluciones tecnológicas. El paso hacia la fibra óptica debe ser obligado para que Internet continúe avanzando. Sin más velocidad y seguridad jurídica la evolución será mucho más lenta.

Los datos no dejan lugar a dudas. EEUU. es el país donde existe un mayor número de recursos legales y tecnológicos. Si a eso se le une el hecho de un bajo coste en las comunicaciones se entiende la razón por la que existen hoy en día 106 millones de internautas norteamericanos, el 50 % de su población adulta. En Europa apenas llega al 10 %, y en América Latina es aún inferior. En resumen, Internet y el comercio electrónico es una de las mayores revoluciones que ha conocido el mundo, sólo con un rá pido ajuste podremos afrontar el gran reto que supone.

BIBLIOGRAFIA

1. Don Tapscott. The Digital Economy. McGraw Hill; 1995.

2. Frank Barbetta. Infonet and SITA/Scitor - New strategies for a new global market. Business Communications Review. 1996;26(4):32.

3. James Champy, Robert Buday, Nitin Nohria. Creating the Electronic Community. Information Week. June 10, 1996(583):57-64.
http://techweb.cmp.com/techweb/iw/583/csc.htm

4. James Martin. The Great Transition. New-York: Amacom; 1995.

5. T. Malone, J. Yates, R. Benjamin. Electronic Markets and Electronic Hierarchies. Communications of the ACM. 1987;30(6):484-497.

6 Thomas H. Davenport. Process Innovation, Reengineering Work Through Information Technology. Harvard Business School Press;

7. http://www.internetindicators.com/

8. http://www.nua.ie/surveys/index.cgi

Globalizacion e Informática Jurídica: El Desafío del Notariado

Dr. Carlos Ferreyros Soto (Perú)

- ✓ Consultor Internacional.
- ✓ Gerente de Informática del Poder Judicial
- ✓ Asesor del Congreso de la República del Perú
- ✓ Gerente del Objetivo C Magistrados de la Secretaría Ejecutiva de la Comisión Ejecutiva del Poder Judicial.
- ✓ Gerente de Planificación de la Secretaría Ejecutiva la Comisión Ejecutiva del Ministerio Público.
- ✓ Director de Sistematización Legislativa del Ministerio de Justicia.
- ✓ Ex Presidente y Actual Miembro de la Comisión de Informática y Telecomunicaciones del Colegio de Abogados de Lima, Perú.
- ✓ Doctor en Derecho e Informática de la Université de Montpellier I, France.
- ✓ Máster of Science de Desarrollo de l'Institut Agronomique Mediterranéen de Montpellier, France.
- ✓ Abogado de la Universidad Nacional Mayor de San Marcos, Perú.
- ✓ Licenciado en Sociología de la Universidad Nacional Mayor de San Marcos, Perú.

RESUMEN: Los imperativos de la globalización y de los cambios tecnológicos puede entrañar modificaciones substanciales en la forma de organizarse y de producir de la sociedad. Particularmente, con la informática de gestión y los sistemas expertos o de ayuda a la decisión se puede modificar la manera de producir actos jurídicos o notariales. Ello conlleva a plantearse una serie de modificaciones que debieran ser propuestas por los juristas y notarios a fin de adecuar sus normas y organizaciones al nuevo orden internacional y a los nuevos cambios tecnológicos.

ABSTRACTS:Globalización / Tecnología / Informática / Telemática / Informática Jurídica / Informática Documental /Informática de Gestión / Derecho / Derecho Informático / Sistemas Expertos / Sistemas de Ayuda a la Decisión /Campos Fijos / Campos Variables / Comercio Electrónico / Correo Electrónico / Internet / Notarios / Fedatarios Informáticos / Firma Digital / Firma Electrónica /Registro Público / Minuta /.

1. GLOBALIZACION Y CAMBIOS TECNOLOGICOS

La tesis principal de los teóricos de la globalización es que el mundo estará cada vez más interconectado. Merced a ello, la comunidad de valores culturales, económicos y sociales nos conducirán a una gran aldea global.

Sin embargo, el fenómeno de la globalización proyecta una imagen doble: primero, "...que gracias a la tecnología y al mayor acercamiento entre seres del mismo planeta, verá solucionados los principales problemas que hoy aquejan a la humanidad: el hambre, el deterioro ambiental y la pobreza; segundo, apocalíptica, que predice a un ser abandonado al ocio tecnológico dependiente y ultra materialista".[1] Otras opiniones recuperan en la globalización, el carácter de menor o mayor desarrollo tecnológico.

La opinión de Fernando Henrique Cardozo, nos parece las más acertada cuando se refiere a los temas referidos a la globalización. Precisa bien que el fenómeno es mucho más amplio: "...son las cuestiones globales las que están al orden del día y que contienen verdaderas revoluciones en nuestro siglo. La revolución de la Universidad, la empresa y la representación democrática, dicho de otra manera, de la ciencia, la tecnología y de la libertad...".

Ello replantea implícitamente el problema de la dominación - dependencia de las naciones y países cuanto al acceso, uso o ejercicio de la ciencia, de la tecnología y de la libertad.

[1] Alfredo PAINO SCARPATI El Notario frente a la globalización de las economías nacionales. Notarius Revista del Colegio de Notarios de Lima, Año V, 1995, N° 5, pp. 47-52.

Las diferencias actuales entre los representantes de los países pertenecientes al ex GATT y los actuales referidos a la Organización Mundial de Comercio, sobre los temas referidos a la Excepción Cultural - inclusive entre aquellos de similar grado de desarrollo -, no hacen sino confirmar los efectos que la empresa, el comercio, la tecnología puedan vehicular una imagen cultural mayoritaria de aquellos países o empresas y negar otras formas culturales igualmente valiosas. Ello haría desaparecer la enorme riquezas de las minorías.[2]

Por ello la globalización tendrá consecuencias importantes respecto del individuo, del hogar, de la empresa, del mercado, del mundo. Cuanto al individuo, la globalización permitirá que este acceda, si dispone de los medios necesarios, a la información y a su forma más elaborada: el saber. El hogar no estará más marcado por las determinantes físicas del espacio y por los principios de privacidad e intimidad relativas a la familia sino que en él convivirá frecuentemente el ámbito de trabajo o de la empresa. La empresa será marcada por una mayor agresividad competitiva pero de género diferente, no será el tamaño de las unidades productivas que marcará la diferencia sino su grado de innovación, de eficiencia, cuyo principal componente será el capital intangible y su forma de gestión más aceptada: aquella que revalore el factor humano y la naturaleza. El mercado será de envergadura mundial, sin fronteras con volúmenes enormes de intercambio y de velocidad en las transacciones por efecto de la interconexión. En el Mundo, los países y las empresas transnacionales basarán su liderazgo en el poder de la información y de los datos. [3]

A estos factores, es necesario integrar uno nuevo: el relativo a la inflación de la información. Según ciertos autores[4], se viene produciendo desde hace algunos años una mayor y más densa producción de la información legislativa, de los datos, de las imágenes, del sonido, vinculado, es cierto, a las nuevas tecnologías relacionadas con ellos: la informática, la burótica, la telemática; pero también al deseo de regular de manera mas extensa y precisa los derechos y obligaciones de las personas y del Estado. Estos factores contribuirán significativamente a la creación, ejercicio o modificación legislativa.

Ahora bien, las grandes revoluciones tecnológicas se han acompañado, históricamente, de frondosas regulaciones legislativas y jurídicas a fin de proteger el objeto de éstas, el entorno de aplicación como también permitir la educación del usuario. El ejemplo de la última gran revolución tecnológica: la del automóvil, nos recuerda la enorme producción de normas, leyes, reglamentos que fueron necesarios introducir en la cultura mundial: Códigos y Reglamentos de Tránsito, de Pasajeros, de Carga, de Señales, de Seguridad, de Medio Ambiente, de Construcción de Carreteras, Pistas, Veredas, de Peatones, de Policía,...

Por ello, la revolución informática, imbricada con una segunda, de las telecomunicaciones, según Alain MINC Telemática, hace que sea necesario un similar o mayor despliegue normativo, no solamente cuanto al instrumento físico, el continente de la informática y de las telecomunicaciones, sino de su contenido: la información, los datos, las imágenes, el sonido.

Históricamente, las llamadas revoluciones tecnológicas apuntaron a mejorar o potenciar las limitadas capacidades, primero físicas, del hombre. En principio, aquellas relacionadas con la energía, potencia, fuerza, para luego trasladarse a aquellas referidas a los sentidos: visión, audición, olfato, tacto, gusto. Ahora, las revoluciones tecnológicas se orientan a mejorar o potenciar las capacidades mentales del hombre: la memoria, la comunicación, el cálculo, la asociación lógica. Estas revoluciones obedecen al contexto socio cultural, como del interés del hombre en cada época. La supervivencia, la rentabilidad, el control...

La informática representa ahora esa remarcable herramienta tecnológica capaz de potenciar las tareas propias del cerebro, la voz, la escritura, el lenguaje, la comunicación. Por ello es particularmente importante para el ejercicio de la función del jurista, pues las características propias de la informática: memorización, comunicación, cálculo y asociación lógica, son imprescindibles para el memorizar y archivar las normas, analizar el lenguaje y el discurso lógico contenido en ellas, contabilizar y comunicar estas.

---

[2] Cabe agregar a ello, las dificultades de la Unión Europea que reúne a quince países de Europa, cuyas autoridades han pospuesto la integración del capítulo referido a la Justicia.

[3] Alfredo PAINO SCARPATI. OP. Cit. pp. 47-52.

[4] Entre ellos, Henri MANZANARES, et Philippe NECTORUZ, "L'informatique au service du juriste" Editoriale LITEC 1988, Paris, France. Leonidas KANELLOS, "L'inflation juridique" These Doctorale, 1992, Montpellier, France.

Sin embargo, no es solamente que estas características informáticas están disponibles en el ordenador sino porque cuantitativa y cualitativamente estas actividades se desarrollan a altas velocidades, en volúmenes impresionantes, incrementando los ratios de producción y los índices de productividad en las tareas jurídicas. Así, pueden ser almacenadas y recuperadas de la memoria del ordenador o del computador, no solo innumerables resoluciones, documentos, escritos, sino que estos pueden ser normalizados, modelizados, para su uso discrecional. Esta información puede ser, además, comunicada de o a diferentes puntos del país o del mundo al instante. Igualmente puede servirse del cálculo, y prepararse o tratarse la información lógicamente del discurso o del argumento legal, jurídico.

De otro lado, la técnica informática, al disponer de un lenguaje binario particular, sobre la base del cual se construyen los algoritmos o instrucciones para un determinado fin aplicativo y vehiculado a través de impulsos electromagnéticos, presenta desafíos importantes para la regulación de esta vertiente inmaterial por el Derecho.

De ello se desprende que esta nueva técnica informática se imbrica en una doble relación con el Derecho: en las aplicaciones informáticas orientadas al ámbito jurídico, y en la regulación de la informática por el Derecho. A la primera relación se le ha quedado en llamar Informática Jurídica y a la segunda, Derecho de la Informática. Ambas se encuentran estrechamente ligadas y forman parte de las inquietudes científicas, académicas, profesionales, técnicas que marcan esta relación.

La Informática Jurídica tiene entonces por objeto, identificar, crear, explotar aquellas aplicaciones informáticas que pueden ser de uso del jurista: base de datos legislativas, doctrinales, jurisprudenciales, o aplicativos de gestión documental, válidos tanto para el ámbito jurisdiccional común, privativos; como de gestión de Estudios de abogados, notarios; inclusive de seguimiento de denuncias, de demandas, expedientes, o registros de antecedentes judiciales, de condenas, entre otras.[5] Cuando estas aplicaciones son concebidas por los INFORMATICOS Y LOS PROFESIONALES DEL DERECHO, pueden ser herramientas bastante bien adaptadas para resolver los problemas derivados del quehacer de los informáticos, los juristas, la gestión y la administración de justicia. Sus principales triunfos serán los relativos a la eficiencia, eficacia, seguridad, pertinencia, rapidez, necesarias a cada una de estas empresas.

La informática, y por ampliación la telemática, tienen por objeto el estudio de la regulación de esta disciplina por el Derecho. Así, las diferentes ramas que componen el Derecho: penal, civil, laboral, constitucional, u otros, en los cuales, en los cuales interviene un elemento de naturaleza informática, podrá ser materia de regulación clásica o sui generis. En el caso penal, ya se presentan con bastante frecuencia algunos delitos que pueden ser cometidos por intermedio de la computadora. En algunos casos será posible utilizar los instrumentos del derecho común, en otros, es posible que la especificidad informática sobrepase y altere la definición tradicional de los tipos o elementos constitutivos del delito, o al menos replantee estos. La diferencia evidente que existe entre una falta y una delito en medio material, sin la intervención del elemento informático puede ser más sutil si la miramos desde la perspectiva del instrumento informático en medio inmaterial. O el desplazamiento de la "cosa", en los casos de hurto o robo, si se realiza o no por medios informáticos.[6] Igualmente, si nos referimos al dominio civil, en relación a los bienes informáticos materiales creados y la definición, originalidad o propiedad de estos. Inclusive, en materia laboral, replantea cuestiones aún novedosas relativas a las condiciones de trabajo del operador frente al computador, el teletrabajo o los problemas generados por la informática y la sindicalización; o finalmente en materia constitucional, los Recursos de Garantía como el Habeas Data, y la aparente contradicción frente al derecho o ejercicio legítimo de la violencia por el Estado, o los derechos a la privacidad e intimidad de las personas, en el caso de datos e informaciones.

Actualmente el lado más dinámico de la relación informática y derecho, la informática jurídica, gracias a las características de telecomunicación y de las nuevas tendencias reguladoras que aparecen, la información contenida en soportes electromagnéticos y otros complementarios podrá ser compartida y analizada por los diferentes juristas en el país y el mundo.

---

[5] Carlos FERREYROS SOTO, " L'automatisation de l'instruction pénale ordinaire au Pérou. Analyse et propositions". Tesis Doctoral presentada en la Université de Montpellier I, Faculté de Droit, Octubre 1992, 606 pp.

[6] Carlos FERREYROS SOTO, "Aspectos Metodológicos del Delito Informático". Publicado en Informática y Derecho N° 9, 10, 11. Actas del II Congreso Internacional de Informática y Derecho. Universidad Nacional de Educación a Distancia de Mérida, España. 407- 412. 1996

Ello perfeccionará ciertamente el enfoque sobre el derecho comparado, sus instituciones y las incidencias que éste tendrá en el futuro en la regulación supranacional y en los efectos sobre la economía, la educación, pero también sobre cultura, la nacionalidad, la soberanía. Pero sobre todo, se percibe que los fenómenos de globalización, mundialización, vinculados a los procesos de desarrollo del "bien informacional", confirman la tendencia de mayor desarrollo en estos sectores, de creciente rentabilidad, pero contrariamente, aún inadecuadamente regulados. Lo que planteará nuevos retos cuanto a la investigación y el desarrollo futuro de la humanidad.

2. INFORMATICA JURIDICA Y DE GESTION

El rol del jurista, abogado, notario frente al fenómeno de la globalización es un tema de interés actual no solo por sus consecuencias el ámbito nacional como internacional.

Hasta poco antes del advenimiento de la informática, una de sus preocupaciones mayores fue la de establecer documentos normalizados, dotarse de bases de datos legales e informaciones que permitan la elaboración, seguimiento y control en el desarrollo y la celebración de sus actos. Estos documentos se desagregaban, resumo: por tipos de actos, de control ordinal, nominal, situación del trámite, seguimiento, fechas de entrada/salida, por responsable, por cliente, entre otros criterios. Indirectamente, les permitía dar cuenta del cumplimiento o no de los requisitos legales, judiciales, notariales, de accesos o bloqueos en la celebración de los actos, de control de llegadas y salidas de documentos, de las diferentes solicitudes, de las normas aplicables, de las formalidades. Estas aplicaciones, automatizadas se inscribieron en la llamada *Informática Documental.*

Mas tarde, al evolucionar las aplicaciones informáticas al ámbito jurídico se diferenció la *informática documental* de la *informática de gestión*, según la menor o mayor recuperación y pertinencia de los datos y las informaciones. Así se pudo avanzar en otra concepción del desarrollo de aplicaciones jurídicos - notariales. De las aplicaciones de la *informática de gestión* que tienen por objetivo recopilar, crear, comparar, editar, administrar, documentos, datos e informaciones se pasó a los *sistemas de ayuda a la decisión*, y ahora a los *sistemas expertos*. La principal realización actual de estos últimos es la *redacción automática de actos jurídicos, notariales.*

La finalidad última de la *redacción automática de actos jurídicos*, no es la de organizar o duplicar los mismos documentos que pueden reproducirse por medios mecánicos o automáticos, como en la *informática documental*, sino elaborar proposiciones lógico-matemáticas, basadas en datos e informaciones seleccionados, y/o en el discurso normativo del jurista, abogado o notario. Estas proposiciones relacionan los datos e informaciones y/o el discurso normativo bajo la forma de una aplicación informática, la cual al ponerla en marcha, evalúa las alternativas posibles para cada acto, selecciona éstas y elabora el acta o minuta pertinente.

La diferencia entre la *informática documental* y la *informática de gestión*, estriba en la calidad del acopio, tratamiento, recuperación, pertinencia y difusión de los datos, informaciones y discurso normativo. Como también del análisis lógico, lingüístico y social de cada una de las variables tomadas en cuenta para los actos jurídicos o notariales. Y obviamente, de los conocimientos de los cuales dispone el agente del análisis para la concepción y selección de las proposiciones lógico-matemáticas en la elaboración del acto legal, jurídico o notarial. Si extrapolamos, estos conceptos legales, jurídicos, notariales que hemos abordado al ámbito económico, hablaríamos del mayor o menor valor agregado en la búsqueda y recuperación de las nociones requeridas, según se trate de *informática documental* o de *informática de gestión.*

En la *informática documental*, se disponen las unidades de documentos, uno a uno, sin relación a un análisis sistémico, identificándole por un número o una función. Así, podrá ser posible de obtener los formularios, fichas, modelos, necesarios para la realización de UN determinado acto. Cuanto a su resultado, es posible, que las aplicaciones informáticas sean capaces de dar cuenta de su número, orden, avance, pero gracias a su enumeración o función principal del documento, formulario o modelo, como también por la vocación o contenido de un programa informático; no obstante, cada acto es independiente del otro, repetitivo, rutinario, estadístico.

En la *informática de gestión*, la selección de las nociones o argumentos legales, jurídicos, notariales a tratar, su-

bleva tres tipos de análisis: el lógico, a fin de identificar las proposiciones y premisas contenidas en las informaciones y discurso jurídico. El lingüístico, a fin de diferenciar en la lengua y en el lenguaje las nociones pertenecientes al lenguaje natural y al lenguaje jurídico, no solo cuanto a la univocidad o multivocidad de los conceptos, sino cuanto a la sinonimia, la antinomia, la polisemia. Finalmente, en el social, con el auxilio de la antropología y sociología, a fin de evaluar la correspondencia y vigencia de las nociones, términos o conceptos utilizados en función del tiempo, la cultura, los grupos... Además, en la *informática de gestión,* cada noción, unidad del documento o acto: llámense datos, informaciones, normas, son analizados sistemáticamente. Estos datos, informaciones y normas, están ligados entre sí. Es decir, forman un sistema de variables interdependientes, de multicriterios y de incalculables alternativas, que pueden ser administrados por un Programa Informático, el cual posee sus propias potencialidades de presentación, numeración, tratamiento, análisis u organización. Así, en la *informática de gestión para el ámbito notarial, es a partir del análisis de los datos, informaciones y normas que puede generarse un sistema experto o de ayuda a la decisión el cual puede elaborar o ayudar a elaborar, el documento o acto jurídico o notarial. Con - o sin - el concurso del cuerpo técnico y del Notario, quienes supervisan - o auxilian - y controlan el desarrollo y la pertinencia del mismo y con el apoyo del programa informatizado, sobre el cual se soporta la aplicación informática.*

Aparentemente las unidades de *tiempo* que demanda la concepción, análisis y elaboración de aplicativos en la *Informática documental* es menor que en la *Informática de Gestión.* Sin embargo, una vez identificados el Programa Informático y realizados los análisis pertinentes de datos, informaciones y normas en su triple vertiente lógica, lingüística y social, el tiempo de redacción del Acto Jurídico o Notarial, es infinitamente menor y más fiable porque: los campos fijos[7] para cada acto son elaborados automáticamente e integrados en el acto notarial. Los campos variables[8], son propuestos al agente de la elaboración del acto, como elementos de ayuda a su decisión o como elementos *sui generis.*

La tendencia actual, por consideraciones de comodidad, empresariales, económicas, como por las leyes de oferta y demanda en el mercado de los profesionales del Derecho y del Notariado, es al uso ampliado de la técnica de *redacción automática de actos jurídicos.* Existe igualmente un criterio que llamaremos de seguridad jurídica, compuesta por criterios de pertinencia, racionalidad y de seguridad propiamente tal en la redacción de los actos notariales o jurídicos, por la cual, aún incrementando la producción y productividad de estos: se puede producir mejor y mayor cantidad de actos jurídicos y notariales en una misma unidad de tiempo, siendo más seguros en su elaboración, recuperación, pertinencia, transmisión y difusión.

Estas variables endógenas a la realización del acto jurídico o notarial no se encuentran exentas de una variable exógena: el Nuevo Marco Legal Mundial y Nacional. Este Nuevo Marco Legal Mundial, incidirá en los aspectos que la tecnología telemática determina. En el Derecho Constitucional, al sustentarse las nuevas tecnologías en el individuo, deberán reforzarse entonces las áreas relativas a sus derechos fundamentales y a sus garantías individuales, prioritariamente, en lo relativo a sus derechos relativos al acceso a la información y al saber. Creo que tres áreas del Derecho sufrirán sustantivos cambios derivados de estas tendencias. En el Derecho Comercial, el auge mayor será el relacionado con los intercambios electrónicos - el comercio electrónico en particular. En el Derecho de Contratos, la multiplicidad de nuevas modalidades de intercambio y de relación económica que ello sugiere, por la masificación e inmaterialidad del medio, supondrá proponer nuevas alternativas de identificación, seguridad y prueba. En el Derecho Notarial y Registral, la concepción de nuevas formas de solemnidades de fijarse éstas, de identificación y de acreditación, conllevará innovativas maneras de formalizar los actos. La necesidad de inscripción de los actos y bienes; de la actualización y publicidad de los Registros, de desmaterialización de los títulos, supone crear nuevas formas que otorguen igual o mayor fiabilidad y seguridad que en soporte material, físico. Concomitante con ello, se exigirá una similar adecuación de los Códigos Adjetivos, particularmente, en los nuevos elementos probatorios.

---

[7] Puede definirse como los datos, conceptos, nociones, que son invariables en la elaboración de un Acto jurídico o notarial: puede ser : una misma dependencia a la cual se remiten los actos, una misma norma aplicable a un mismo acto...

[8] Se dice de los datos, conceptos, nociones que son variables en la elaboración de un Acto jurídico o notarial: puede ser : el nombre de las personas que varían de un Acto a otro, los identificantes de documentos de una persona natural o jurídica a otro...

De manera general, el Mundo debiera encaminarse hacia nuevas y más estandarizadas formas de regulación mundial. El papel de la influencia económica, cultural o zonas de influencia estratégica regional, será uno de los criterios principales para la uniformización de normas. Las actuales tendencias de integrar Bases de Datos Legislativas sobre temas motores, como Códigos Penales, criminalidad organizada, trafico ilícito de drogas, comercio de armas, lavado de dinero, terrorismo internacional, no son sino incipientes formas de ampliar nuevas figuras delictivas de regulación y aplicación válida a los países que integran estos bloques. Por ello, el Derecho de Integración y el Derecho Comparado, serán dos vectores importantes en la consolidación de esta tendencia.

El Nuevo Marco Legal Nacional, tiene en la Política del Estado en materia Judicial su principal instrumento de regulación. Son sus Organos Legislativos y Ejecutivos los que tienen la facultad de regular el corpus judicial, incluyendo el notarial. Ellos definen su número y currícula de formación; identificación y regulación de los actos practicados por estos cuerpos profesionales del Derecho; señalan los Distritos Judiciales, Notariales y la afectación individual en el espacio geográfico; fijan las tasa y aranceles respectivos, entre otros. Esta variable de Política Nacional incide enormemente sobre la cantidad, la calidad, y la fijación de la mayor o menor competencia y jurisdicción en la elaboración de los Actos Judiciales y Notariales en los diferentes Distritos Judiciales.

3. DESAFIOS DE LA INFORMATICA JURIDICA: EL CASO DEL NOTARIADO

Si una aplicación de *informática documental* es capaz de producir una base de datos indicando cual es la situación del trámite de un expediente, su número, las personas que intervienen, los tipo de acto, los responsable, u otros criterios las unidades de tiempo para su elaboración disminuyen en el seguimiento y memorización con relación a los sistemas manuales o mecánicos. Si comparamos ésta tecnología intermedia con aplicaciones relacionadas a la *informática de gestión*, capaces no solamente de dar cuenta o ejecutar todo lo anterior, sino también de elaborar los actos notariales, libre de errores, mecanografiados, en mucho menor tiempo..., obviamente, el rendimiento y excedentes de las Notarías aumenta. Esto configura una nueva relación de menor o mayor potencialidad según se trate de la gestión manual o mecánica de una Notaría, de aplicaciones relacionadas a la *informática documental* o de aquellas relacionadas a la *informática de gestión*, sin mencionar el diferencial que puede generar el material y equipo de mayor rendimiento, o de personal formado a una u otra técnica. Obviamente, los costos en la composición técnica u orgánica del capital son diferentes.

En las aplicaciones *informáticas de gestión*, los programas informáticos contienen las *"biblias"* de actos, es decir, el inventario de actos jurídicos o notariales potenciales, los cuales pueden abarcar la redacción del correo tipo, de actas de compromiso, de contratos, de sociedades, de matrimonios, de donaciones, de sucesiones, de venta, de préstamos, de actos diversos, por citar los principales títulos. Estos actos están ya predeterminados y sólo son necesarios para su elaboración automática, los ajustes personales del o de los actos, vía los campos móviles. Los nombres de los que intervienen, sus direcciones, sus números de libreta electoral, sus estados civiles, sus participaciones diferentes en la constitución de una sociedad, son algunos de los ejemplos. *Cada una de las rúbricas de la "biblia" puede contener innumerables modelos.* De los cuales, en la práctica se emplean, solo unos cuantos. A ello puede integrárseles en *red interna como externa de comunicación*. Así, ya no es necesario que los clientes se abarroten en las antesalas de las Notarías, basta con el envío o interrogación de la información necesaria mediante teléfono, telegrama, télex, fax, o de comunicación de ordenador a ordenador, vía módems y satélites, a través de cientos de metros o miles de kilómetros, con una ventaja adicional: el ordenador almacena la información en memoria durante mucho tiempo, y puede modificar, cuando así se requiera, sólo aquellos aspectos que así lo exigen, los campos fijos y campos variables, a los cuales nos referimos anteriormente. No es necesario pues para un nuevo acto recomenzar con la exigencia de información o requisitos ya satisfechos: números de libreta electoral, militar, tributaria, dirección, nombre y apellidos, estado civil, si ya se cuenta con aquella información y ella no ha variado.

La *informática Jurídica* en su aplicación al Notariado, permite entonces, acrecentar la productividades y/o mejorar los sistemas de archivo y de seguridad, porque la técnica informática implica un mayor desarrollo de las propiedades de cálculo, comunicación, asociación lógica y memorización del hombre, auxiliándolo para el desarrollo de sus actividades, y en el ámbito notarial-judicial, generando en consecuencia, un mejor y mayor manejo de información y de actos. Esta carga adicional de trabajo supone un *incremento en la renta diferencial producida por las innovaciones incorporadas al Gabinete jurídico o notarial.*

El desarrollo de programas informáticos llamados "inteligentes": *sistemas expertos o de ayuda a la decisión,* se basan en estas referencias; los cuales pretenden con ello una *imbricación armónica entre las aplicaciones informáticas de gestión con el material y equipo utilizado, el personal y los procedimientos y normas ejecutables.*

Ahora bien, los ritmos de *actividades en cada función judicial o notarial están marcados por el nivel de especialización y profesionalización en cada una de ellas,* sustentándose, fundamentalmente, en la división de funciones y en el acceso al conocimiento técnico y/o habilitación formal. Existen al menos dos niveles, más o menos identificados: el o los Notarios, cuando los titulares son varios (el caso de Europa, verbigracia), y el cuerpo técnico, que pueden ser Asistentes con conocimiento científicos o empíricos. Los asistentes, identifican el o los actos demandados, los comparan con la legislación y reglamentos existentes, verifican los requisitos necesarios, establecen la secuencia histórica, revisan los archivos, comprueban las firmas, y en definitiva, producen los pre-actos, a ser refrendados o no por el Notario habilitado. Este, formaliza o no el acto, con las solemnidades exigidas por la normas, con su presencia y/o con su firma.

Como las aplicaciones de la *informática de gestión* disminuyen y rentabilizan el tiempo de las actuaciones de los notarios, se puede identificar dos grandes actividades relacionadas pero diferenciadas a la producción del acto notarial: las *intervenciones personalizadas del Notario,* a las que se encuentra obligado por las normas en la materia; de aquellas en las cuales *no interviene ni directa ni personalmente el titular de la Notaría.* Se *limitan así las innumerables intervenciones del Notario en aclarar, aconsejar o indicar la rutina a seguir por el cuerpo técnico* de aquellas en las cuales participa directamente[9]. Con la *informática de gestión,* ésta información, éste conocimiento último estará contenido en los programas informáticos.

En términos de rentabilidad económica significa que en el cálculo de la renta total, la proporción de la renta diferencial producida por algunos servicios de la Notaría, tiende a elevarse por efectos del uso de las tecnologías: mayor cantidad y calidad de actos producidos por el ordenador versus la máquina de escribir, pero también por el empleo de los programas informáticos que van a realizar funciones similares al del Técnico o Especialista Notarial, pero bajo su control. Así, *el cálculo del costo medio en la producción de un acto, se establecerá ya no en función del tiempo del especialista que prepara el pre-acto, en su integridad, o del promedio de tiempo del grupo de especialistas que participan en cada frase o secuencia de la elaboración del acto, sino más bien, de la producción personal del Notario.* Así, los índices de soportabilidad de la atención del Notario para responder armónicamente a las demandas de los clientes y del cuerpo técnico tiende a elevarse, fijando sus límites, a partir de ese momento, primero, por los rendimientos de los programas informáticos, más el material y el equipo informático existente, más la calificación del personal. y segundo, por la disponibilidad del tiempo del titular de la Notaría, su sujeción a las solemnidades y por las intervenciones personales indelegables de su función.

La *intervención de estos nuevos elementos: las nuevas tecnologías, informática de gestión y telemática,* las cuales facilitan una mayor producción y productividad de actos jurídicos o notariales, replantean la cuestión de la *competencia,* es decir, la posibilidad de acceder al mercado potencial de otros clientes circunscritos a diferentes Notarías instaladas en un mismo Distrito Notarial, *por los distintos niveles de desarrollo tecnológico* que ellas poseen, y por la *renta de ubicación.* Obviamente, los Estudios Notariales o Jurídicos, mejor dotados informáticamente y mejor ubicados pueden establecer índices de competitividad mucho más altos que aquellos que no lo están, sobre todo, si los baremos arancelarios por acto notarial o judicial se mantienen sujetos a regulación. El incremento de hasta doscientos nuevos despachos notariales, recientemente, se inscribe en ésta igualmente lógica.

Contrariamente, con la *informática de gestión,* así como los nuevos útiles tecnológicos, principalmente *telemáticos, comercio electrónico, internet,* se pone en tela de juicio los criterios de *renta de ubicación*: definidos por

[9] Por el elevado nivel de desarrollo de los medios tecnológicos, cada vez más es mas intermediada la función del jurista o del notario de acreditar o dar fe de los actos en los que participa. Lo que para ellos era posible antes, de ser captado y validado por los sentidos, no lo puede ser más. A fin de suplir o compensar estos sentidos, el hombre utiliza una serie de artefactos y herramientas capaces de "sentir" por el hombre y dar fe de estos actos. Este carácter intermediario de producir fe notarial, hace que cada vez más utilicemos nuevas tecnologías para verificar lo que nuestros sentidos no pueden percibir, y que por lo tanto no pueden acreditar de manera directa. Otros comentarios se refieren a la dificultad que el notario pueda adaptarse al cambio, por lo hierático de sus principios y tradiciones, como por los desafíos de celeridad y volumen de los intercambios. Estas tendencias podrían redifinir un rol del notario en el nuevo orden internacional.

el próximo acceso a centros comerciales, administrativos con fuerte demanda potencial de servicios de Notarías, cuyos criterios definían la ubicación definitiva del negocio; pero de otro lado, atenta contra dos principios notariales al aumentar el riesgo y la formalidad.

Así, ahora es técnicamente posible que cualquier Notaría de Lima pueda realizar actos notariales mediante aplicativos basados en sistemas expertos o de ayuda a la decisión, con cualquier cliente domiciliado en cualquier Distrito Notarial del país o del extranjero, utilizando un Portal, correo electrónico, apelando a la identificación y reconocimiento de los solicitantes por instituciones garantizadas, sin desplazamiento físico de estos, acreditando su voluntad por medio de firmas digitales o electrónicas, abonando sus derechos mediante transferencia en cuenta corriente electrónica y registrándose en los archivos electrónicos de los Registros Públicos correspondientes, y recurriendo a fedatarios informáticos para la recepción de los testimonios de las Minutas respectivas. Este proceso todavía no se realiza de forma integral en el Perú, por ahora. Consideraciones de tipo normativo, de disponibilidad técnica, de seguridad o de reflejo cultural, no lo permiten completamente. Pero, es esta la tendencia hacia la cual se orienta este gran fenómeno de la globalización y de cambios tecnológicos.

Por ello, los juristas, y en particular los notarios, debieran proponer y participar en el esfuerzo de adecuar sus normas y organizaciones a los nuevos retos que emergen del doble movimiento: de construcción del nuevo orden internacional y de generación e incorporación de nuevos las nuevas tecnologías.

Lima, Abril 2000

El Impacto de la Era Digital en el Derecho

Por Cristian L. Calderón Rodríguez (Perú)

INTRODUCCION

La aparición del papel y por supuesto la escritura sobre el mismo fue un cambio que revolucionó la comunicación social y sobretodo la forma de garantizar el intercambio de bienes en una sociedad. Gran parte del mundo se desarrollo bajo el paradigma de la escritura sobre un papel. En el mundo de la ciencia también encontramos cambios en el paradigma que permitió el avance de la ciencia, basta recordar a Galileo Galilei – sin embargo se mueve- y a Copernico, quienes resquebrajaron los modelos científicos de aquellos que afirmaban que la tierra era el centro del universo y que todo giraba en torno a esta. En el campo de la fe, Jesucristo revolucionó el paradigma religioso al sufrir como hombre, morir y resucitar, cuando en el mundo antiguo la existencia del politeísmo y de los dioses domésticos- llamados lares por los romanos- era el común denominador en la religiosidad de los seres humanos. Tan grande fue el cambio originado por Jesucristo que dividió la historia de la humanidad en antes y después de su existencia terrenal.

Hoy en día la humanidad, se encuentra inmersa en un cambio de paradigma, las formas tradicionales de obtener información, publicitar bienes, realizar transacciones, han sido resquebrajadas y superadas por el uso de medios tecnológicos que antes no existían.

Ello ha llevado a que los economistas denominen a este nuevo paradigma como economía digital, también ha obligado a que las Administraciones publicas lo utilicen como modelo para la reforma del estado, y que los educadores se sientan amenazados por el computador si es que no se reestructura su misión en la escuela.

EL PAPEL DEL DERECHO EN EL MUNDO VIRTUAL.

El Derecho también se ve afectado por estos cambios sociales, solo que la intensidad y el grado del giro, superan ampliamente lo ocurrido luego de la revolución francesa o la revolución industrial. La imagen del Abogado casi siempre se ha asociado a un papel o un libro, o a una pluma de escribir, o a un maletín, aunque algunos ya los asocian con el teléfono móvil en uso constante.

Pues bien no solo es la imagen del Abogado la que se asocia al medio escrito, sino que el Derecho mismo se sustenta en el uso y abuso del medio escrito, incluso algunos contratos tienen dicha solemnidad bajo sanción de carecer de efectos jurídicos. En el medio procesal se utilizan aforismos como "lo que no esta en el expediente, no existe en el mundo" y en el argot popular la frase "me han empapelado" denota el fastidio de recibir documentos de incidencia legal para una persona. La prueba por excelencia para acreditar una transacción es el papel con firmas manuscritas de las personas que intervienen.

Sin embargo el paradigma del documento escrito con firmas manuscritas esta siendo dejado de lado por el uso del documento digital con o sin firma electrónica sobre el mensaje. Las transacciones, la publicidad y la información se viabilizan en un formato ajeno al medio escrito. Para muchas personas incluyendo a las empresas el cambio de paradigma significa una facilitación en la búsqueda de información, acceso a mercados mundiales, a nuevas tecnologías e incluso facilita la compraventa de mercancías. El cambio hacia el mundo digital es relativamente bajo en comparación con los beneficios que este ofrece, en consecuencia el uso de tecnologías de la información no es tan traumante para el común de las personas, como lo es para el mundo del Derecho.

Para el ordenamiento legal, el uso de tecnologías de la información se convierte en un uno de los mayores retos que tiene que enfrentar y superar, si es que quiere cumplir con sus objetivos de establecer las reglas de convivencia social.

El Derecho tiene que tener las respuestas adecuadas para facilitar la transición del medio físico al mundo virtual, de lo contrario la convivencia social en Internet sería una suerte de anarquía que puede llevar a su propio aniquilamiento. Claro esta, que todo ordenamiento legal surge cuando existe un grupo social, y de hecho en Internet ya existen reglas de convivencia y códigos de conducta que están regulando a la mayoría de los internautas. Lo que sucede en Internet es que los propios actores tienen internalizadas sus normas y no la toman como impuestas por terceras personas, tal como sucede con algunas comunidades campesinas respecto al derecho occidental.

El reto del Derecho es, pues, flexibilizar sus instituciones e incorporar aquellas normas surgidas dentro del Internet para que todos los actos jurídicos que se den dentro del mundo virtual tengan idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios tenga los mismos efectos legales.

Por tanto resulta de suma importancia revisar nuestros ordenamientos jurídicos y reorientarlos hacia la esfera digital tal cual lo vienen haciendo las administraciones gubernamentales, empresas y personas de todo el mundo. Nosotros no somos de la opinión de "crear" una nueva rama del Derecho, como es el Derecho Laboral, o el derecho Penal, puesto que el cambio atraviesa a todas las especialidades jurídicas, con distintos niveles de afectación, es decir, no pretendamos definir el objeto de estudio de esta "especialidad" porque no existe como tal. Este cambio subyace a todas las especialidades del Derecho.

Cabe mencionar que no debemos confundir lo expresado con la aparición del Derecho informático que si tiene un objeto de estudio, sin embargo en la medida que el cambio se generalice y en la medida que el objeto de estudio de esta especialidad aumente, su importancia en la nueva configuración del Derecho va ser muy valiosa. Su importancia será equivalente a la que tiene el Derecho Civil para el sistema romano – germánico. Para aquellos lectores que pertenecen al sistema del Common Law, el sistema que predomina en América Hispana es el sistema de codificación o sistema romano – germánico, donde el Derecho Civil codificado en un solo cuerpo legal irradia sus efectos a las demás áreas del Derecho.

Ante ello nos surge la pregunta si la actual convergencia digital de la sociedad puede originar la creación de un sistema jurídico propio o unificar los ya existentes, el tiempo nos lo dirá, lo es cierto es que los cambios actuales modificarán los sistemas jurídicos ya existentes en el mundo.

PRIMER PASO: ¿ POR DONDE EMPEZAMOS?

A nuestro entender las sociedades se organizan desde los principios y reglas estipulados en la Carta Magna, de esta se desprende el resto del ordenamiento jurídico. Sin embargo para llegar a una modificación del pacto social que implica la aprobación de una modificación constitucional, es necesario que exista un movimiento social que sustente y que exija los cambios en la Carta Magna de un país. Así sucedió con la Revolución francesa, con el movimiento obrero en Weimar (1919) y con el movimiento liberal en el Perú a inicios de los 90's(1993). No es ilógico pensar ni pregonar que en un futuro próximo el acceso a la Internet debe ser un derecho constitucional de todo ser humano, y contra la negativa injustificada de imposibilitar el acceso a la Internet se pueda interponer una acción de amparo. Sin embargo hoy en día la legislación sobre la tarifa plana sigue siendo un tema de discusión en algunos países como el nuestro. Lo cual demuestra que las demandas del sector digital aún no cobran la fuerza necesaria.

El Derecho en forma aislada empieza a adaptar sus instituciones a la era digital, algunas veces en forma errónea o insuficiente, pero cada vez las normativas especiales empiezan a generalizarse y aplicarse a otras áreas del Derecho. Vemos que en el caso Peruano la Aduana fue la pionera en establecer procedimientos administrativos digitales, mediante el uso de claves publicas designadas a los agentes de Aduanas. La legalidad de estos procedimientos - basados en formatos EDI-, se amparan en la Ley General de Aduanas y en su reglamento (1996). Posteriormente otras entidades publicas comenzaron a brindar sus servicios vía la Internet (registros públicos de Lima y Callao).

Estos avances en el Derecho no significa que el proceso sea unilateral y sencillo, por el contrario en el año 1999 la Aduana del Perú emitió un procedimiento que desvirtuó la eficacia del mensaje electrónico tal como se había colocado en la Ley y el reglamento. Ello obligó a que se presentaran escritos de apelación ante tal decisión, y en este año el Tribunal Fiscal en una jurisprudencia de observancia obligatoria para toda la Administración Aduanera recogió la posición de los exportadores y dejo de lado el procedimiento de la Aduana en razón que desnaturalizaba lo dicho en la Ley General de Aduanas. ¿Que significa esto?, que el cambio no había sido interiorizado en algunos funcionarios aduaneros y que fue necesario corregir la interpretación de la administración para viavilizar el comercio exterior.

Recientemente el Ministerio de Justicia, ha reglamentado un articulo de la Ley de Microfirmas (traslado de un documento a un medio magnético) permitiendo el envío de documentos electrónicos con firma digital. Cabe mencionar que para ello la legislación exige la presencia de un fedatario o notario que de Fe pública de dicho acto. Este avance significa que los notarios que tengan la facultad de dar fe de la migración de estos documentos lo puedan enviar en forma electronica al Registro Publico de Lima y Callao para la inscripción de títulos.

Pues bien en el Perú, como en el resto de América los Parlamentos están estudiando la posibilidad de emitir normas que regulen la contratación electrónica y repriman los delitos informáticos. Esto ha llevado a que en el Perú se cuente con proyectos muy avanzados en temas de certificación, firmas digitales, contratación electrónica, etc.

Del mismo modo, existe en el Perú un centro de arbitraje y conciliación especializado en temas de comercio electrónico e Internet y que utiliza un procedimiento virtual para la solución de controversias. Es decir no solo es la especialización en dicha área sino también el uso de la tecnología en la Resolución de conflictos. Cabe mencionar que el Perú es uno de los primeros países en usar las Uniform Domain Name Dispute Resolution Policy de la ICANN.

Sin embargo temas como privacidad, y tributación son aspectos que por lo pronto no han sido proyectados por nuestra legislación. Nosotros creemos que en este año van a aparecer proyectos regulando estas materias puesto que el crecimiento del comercio electronico obliga a las instituciones relacionadas con estos temas a tomar una postura inmediata.

EL SECTOR COMERCIAL COMO IMPULSOR DEL GRAN CAMBIO.

Muchos de los avances expuestos en líneas anteriores se deben a que el sector empresarial necesitó que el sector estatal adoptará mecanismos ágiles para la prestación de sus servicios, claro ejemplo fue el comercio exterior, sin embargo, hoy en día la tendencia es que las empresas utilizan la Internet para realizar sus operaciones comerciales, ya sea con sus consumidores o con sus proveedores. Es por ello que los temas de firmas digitales, pago electrónico, etc. son las mas solicitadas por este sector empresarial.

Muchas empresas están migrando sus sistemas de abastecimiento y de ventas a formatos electrónicos sin necesidad de la existencia de una Ley. Ello desvirtúa la posición de algunos que piensan que una ley de comercio electrónico fomentaría el uso del mismo, puesto que la existencia de la ley otorgaría seguridad a todas las transaciones comerciales, mas no fomentaría el uso de la Internet.

El Internet se ha desarrollado con sus propios códigos y normas de conducta, y en cierta manera ha tenido el reconocimiento del Derecho tradicional en algunos aspectos.

Nosotros consideramos que una ley de fomento al comercio electrónico o del uso de la Internet es una imposición de un sector de la sociedad sobre el resto de la sociedad que no es necesaria ni es útil, el Internet demanda por si solo un cambio en la estructura misma del Derecho, de lo contrario perjudicaría a nuestra economía.

No debemos olvidar que para la presente década la economía de la Cuenca del pacifico será una de las más atractivas del mundo, en términos de comercio electrónico (b2b) y se estima que el volumen de dinero que circule entre los países miembros de la cuenca será el mas alto del mundo. Por ello, las empresas peruanas deben ofertar

sus bienes y servicios vía Internet en forma segura y tratar de capturar la mayor cantidad de divisas que se transfieran en este sector geográfico. Es por ello, que la legislación tiene que darle la seguridad debida a las empresas para que puedan realizar sus operaciones comerciales.

En cuanto a los servicios de telecomunicación debemos mencionar que es el llamado a revolucionar aún mas la sociedad digital y con ello las estructuras del Derecho, toda vez que los cambios introducidos por las empresas de telecomunicaciones implican una desregulación y una nueva regulación en las concesiones dadas por los gobiernos, al punto que una ampliación tanto en la libertad de sus operaciones como en el ingreso de nuevos operadores sería el camino para revolucionar todo el sistema actual. Vale agregar que las empresas de software también cumplen un papel similar al de las empresas de telecomunicaciones.

La difusión de la Internet a traves del sistema de cabinas públicas implementado por la RCP en el Perú y seguido por cientos de negocios familiares (Pymes) tambien contribuye al cambio social hacia la era digital.

CONSIDERACIONES FINALES

El camino recorrido el Derecho ha sido importante pero insuficiente para los cambios que se vienen en esta era digital, puesto que la aparición de nuevas tecnologías incrementa la necesidad de modificar las estructuras del Derecho en una sociedad. La tendencia del ordenamiento jurídico es pues recoger las normas que los propios actores de Internet utilizan y darle validez jurídica, sin caer en la tentación de regular una tecnología en especial. Estos cambios, impulsado por el sector empresarial, pronto darán frutos en otras áreas de la sociedad como la Educación, la familia, sistema electoral, etc., al extremo que la misma sociedad imponga normas constitucionales que por ejemplo, recojan como derecho fundamental de las personas, la necesidad de acceder a Internet; Que sea una garantía de la administración de justicia que los procedimientos judiciales sean virtuales; Que la creación de personas jurídicas virtuales sea un principio general del capitulo del régimen económico de la Constitución. Como escribiera nuestro querido poeta César Vallejo, "hay hermanos, muchisímo que hacer..."

Nombres de Dominio y Derecho Problemática y Líneas Evolutivas

Marcelo Bauzá Reilly (Uruguay)
Doctor en Derecho. Profesor de Informática Jurídica en la Universidad de la República Oriental de Uruguay

1. LOS ASPECTOS TECNICOS

1.1. El funcionamiento de Internet

Todos aprovechamos lo mejor que podemos la existencia y desarrollo de los llamados sitios www, como así también del correo electrónico y los foros de intercambio y servicio por Internet, que son básicamente los recursos que podemos explotar en la red, más allá de modalidades particulares que ellos asuman. Expresiones máximas, actuales y populares de las tecnologías de la información y comunicación, no obstante el común de las personas conoce poco -aunque sea en su modo más elemental- acerca de las razones por las que funciona correcta y puntualmente toda esta tecnología, dado el voluminoso tráfico de comunicaciones puesto en juego por la misma, a lo largo y ancho del planeta.

En otras palabras, ¿cómo es que los paquetes de datos circulan por la red (tecnología llamada "conmutación por paquetes"), llegando a feliz puerto una y otra vez, a pesar de las distancias a cubrir, y de los nodos que deben atravesar hasta arribar a nuestros propios equipos? He aquí una cuestión técnica a esta altura si se quiere elemental, pero sobre la que resulta necesario reunir algunas nociones suplementarias (siempre básicas), si queremos remontar con cierto conocimiento de causa hacia otros planos de análisis, en particular el plano jurídico.

Es evidente, aún para el profano, que un sistema de comunicaciones como es Internet, de escala mundial y extendido hacia tantas personas y organizaciones, solo puede funcionar correctamente en tanto los equipamientos que intervienen en la operativa se encuentran unívocamente identificados. Así suceden las cosas, efectivamente, en el mundo de las redes globales y las conexiones por Internet. A explicar someramente este punto se consagra el siguiente apartado.

1.1.2. Las direcciones IP

En términos muy simplificados podemos decir que toda máquina llamada a participar en el actual complejo de telecomunicaciones de escala mundial a través de red abierta (sitios web, correo electrónico, forums), debe poseer una identificación unívoca incorporada a su sistema informático. Sólo así podrá verificar su ingreso y participar efectivamente en tales comunicaciones el usuario que se sirva de ellas. Identificación que, para el caso, consiste en una plantilla de números que responden a una cierta codificación.

Con ello, la máquina queda individualizada de modo inconfundible, a todos los efectos pertinentes. Esto permitirá ubicar sitios web y mantener contactos con otras máquinas y redes más potentes en forma transparente para el usuario final, dado que -como se sabe- Internet es una red global compuesta por muchas redes y máquinas servidoras, de nivel local, regional y mundial, que van acumulando y complementando sus prestaciones en forma escalonada. El mecanismo se estructura mediante sucesivos pases y/o autorizaciones de conexión y explotación de esta tecnología (cliente, servidor local, servidor internacional), lo que asegura orden, coherencia y globalidad mundial en las comunicaciones.

Los identificadores técnicos codificados se denominan direcciones IP (por "internet protocol"), y forman parte del conjunto de programas con que se maneja todo el sistema: el llamado protocolo TCP/IP: una especie de sistema operativo para el conjunto de telecomunicaciones de tipo abierto, que funciona bajo el nombre totalizador de "Internet".

Cada dirección IP sirve de guía o punto de referencia, desde el cual parten o llegan los diferentes mensajes. Esto es particularmente cierto para aquellas máquinas que cumplen las funciones centrales en materia de alojamiento y/o distribución de los datos (hosts, servidores, etc.), lugares desde donde vuelven a partir los datos una y

otra vez hacia determinados destinos, en paquetes fraccionados y encaminados por rutas aleatorias (explicación básica pero veraz de esta tecnología).

Así, cuando navegamos en Internet entrando en sucesivos sitios web para leer información, bajar archivos, enviar algún mensaje, hablar y/o escuchar a otros interlocutores (esto también es posible hoy en día como se sabe), etc., estamos operando con estos identificadores o direcciones IP sin saberlo. En pocas palabras, no es más que un sistema que nos posibilita verificar que el contacto buscado es el realmente buscado y no otro diverso. Un contacto que se produce entre nuestra máquina y la multiplicidad de otras máquinas más o menos remotas (o lugares físico-/lógicos de otros sistemas remotos), que están alojando o intermediando la información gestionada en su pasaje y trámite telemáticos.

Las direcciones IP están compuestas por una serie de 4 números, cada uno de ellos poseyendo un máximo de tres cifras, y separados por puntos. Lo que conforma una jerarquía capaz de albergar varios cientos de millones de unidades identificadas (computadoras, algunos periféricos, redes, etc.). Ej. 150.44.300.2., donde cada grupo de números corresponde a un tipo de computadora, red o servicio, y el conjunto conforma una cierta organización técnica que no viene al caso explicar. Basta con saber que se trata de un sistema de escalamiento de posiciones numéricas siguiendo determinados lineamientos jerárquicos, por lo que parte de ese complejo código corresponde a nuestro equipo, otra parte a la empresa o institución que nos provee la conexión a la red, y así sucesivamente hasta llegar a los ordenadores centrales del sistema a escala mundial (localizados en EE.UU). Todo ello según un esquema de ordenamiento cuya complejidad técnica excede nuestras posibilidades de comprensión absoluta.

Lo interesante es tener presente que bastaría con este sistema de identificadores técnicos para que todo funcionase normalmente. Pero aún siendo ello técnicamente posible, no resultaría práctico. El ser humano no es diestro, en términos generales, en cuanto a memorizar y manejar series numéricas. Ya bastante tenemos con los números telefónicos, cuestión más sencilla -por cierto- que el tema que nos ocupa, y que aún así nos demanda instrumentos auxiliares como son las agendas. De ahí que tempranamente se haya optado por poner en práctica un sistema de identificadores (podríamos decir "administrativo" por oposición al sistema de direcciones IP de carácter técnico), que se denomina DNS, por "Domain Name System".

1.1.2. Los nombres de dominio

En última instancia, el DNS es un sistema complementario pero no sustitutivo del sistema de direcciones IP, que facilita el manejo de las comunicaciones por el hecho de que resulta más fácil llamarse a través de nombres evocativos que hacerlo a través de series numéricas. En términos drásticamente resumidos, se trata de una base de datos alojada en un servidor central homónimamente denominado DNS (pero en este caso por "domain name server"), que funciona como "espejo" corresponsal de cada dirección IP.

Sin perjuicio de los vientos reformistas que se aprecian en la materia, a los que luego haremos referencia, el DNS o Sistema de Nombres de Dominio continúa conformado actualmente por dominios de primer, segundo y ulteriores niveles, de acuerdo al esquema organizativo que explicaremos a continuación. Los más importantes en consideración técnica y jurídica son los de primer y segundo nivel.

Los dominios de primer nivel o TLDs, por "Top-level domains", presentan rasgos de generalidad e identifican máquinas proveedoras de servicios de conexión a la red. Estos TLDs están subdivididos en dos categorías, a saber:

A) Los gTLDs, "generic Top-level Domain" o sea dominios de primer nivel genéricos. Van por actividad, según unos criterios históricos estipulados originariamente por los EE.UU, que actualmente están en vías de reforma y ampliación. De momento son 7, y se identifican mediante un punto y tres letras como siguen:

.com entidades comerciales de todo el mundo (gestionado por NSi)
.net servicios de internet (gestionado por NSi)
.org entidades no comerciales de todo el mundo (gestionado por NSi)

.edu educación superior (originariamente universidades americanas; actualmente abierto a todo el mundo)
.mil entidades militares de los EE.UU (gestionado por el gobierno de los EE.UU.)
.gov gobierno de los EE.UU (gestionado por el gobierno de los EE.UU.)
.int entidades internacionales bajo control de la ONU (gestionado por UIT)

B) Los ccTLDs por "*country code Top-level domains*" o sea *dominios de primer nivel por código de* países, que corresponden a un criterio de distribución geográfica estructurado bajo la norma ISO 3166, ya conocido a otros efectos. Estos dominios también utilizan el punto, a renglón seguido del cual se identifica cada país (por excepción también algunas pequeñas islas, antiguos protectorados como Gibraltar, etc., a los que la ONU les ha conferido código ISO). La identificación del caso se especifica mediante las habituales dos letras. Así tenemos, que a Uruguay tiene asignado el dominio .uy, Argentina el dominio .ar, Brasil el .br, España el .es, y así sucesivamente.

Por debajo de estas dos categorías de dominios de primer nivel, se encuentran los llamados dominios de segundo nivel, es decir los SLDs por "Second-Level Domains", dominios de segundo nivel. Y luego están los de ulteriores niveles (tercero, cuarto, etc.), cuya importancia es más bien en planos técnicos internos de cada dirección.

Los dominios de segundo nivel sirven para la identificación de la empresa, institución, persona, producto o servicio que se coloca en el escaparate universal de la red. Sin perjuicio de esta posibilidad, habitualmente se reserva la misma denominación también (dominio de segundo nivel), para establecer una cierta organización funcional de dominios previamente distribuidos en mérito al criterio geográfico (ccTLDs), adosándola a este último y al estilo de lo que sucede en el primer nivel. Esta es una cuestión administrativa variable (reglas nacionales, cuyo ejemplo posterior lo pondrá más en claro), de la que se ocupan las entidades locales que controlan el ccTLDs respectivo. Estas últimas actúan por delegación de funciones recibidas desde el órgano internacional directriz en la materia (actualmente el ICANN). En el caso uruguayo el ente regulatorio nacional es la Universidad de la República, a través de su Servicio Central de Informática Universitario (SeCIU)

Otra manera de comprender este tema, siempre desde un punto de vista exclusivamente técnico, es realizando una lectura de derecha a izquierda. Algunos ejemplos nos mostrarán diversas posibilidades que se presentan:

PRIMER EJEMPLO:

http://www.charona.com Donde encontramos las siguientes partículas:

.comTLDs, en este caso denotativo del tipo de actividad que desarrolla la citada página web (gTLDs), que es de índole "comercial". A esta partícula se la denomina también "sufijo".
.charona Este es el dominio de segundo nivel, que generalmente corresponde a la razón social de la empresa, nombre institucional e -incluso- marcas de productos o servicios. En este caso, se trata de una conocida publicación para niños uruguaya. A esta partícula se la denomina también "radical".
http://www Es de orden puramente técnico. Le indica al usuario que está actuando en el ambiente telemático correspondiente a la web. Se denomina "prefijo".

SEGUNDO EJEMPLO:

http://www.info.juridicas.unam.mxEn este caso, la única diferencia técnica con el ejemplo anterior es que estamos ante un ccTLDs en vez de un gTLDs. Para el caso, el prefijo mx nos indica, conforme la norma ISO 3166, que se trata de una institución de origen mexicano (en efecto, se trata del conocido Instituto de Investigaciones Jurídicas de la UNAM).

Los ejemplos anteriores ofrecen una idea básica de cómo funciona todo el sistema, a partir del modo en que aparece ante los ojos del usuario. En los hechos se observan complejidades mayores de diverso orden. Para comenzar, tenemos la habitual abreviatura del prefijo técnico (www a secas). Asimismo, según adelantáramos antes, es totalmente normal y permitido que existan modificaciones y agregados como para incluir en carácter de domi-

nio de "segundo nivel" algunas partículas que en principio fueron destinadas a identificar dominios de "primer nivel". Esto último se hace por autorización de las entidades internacionales que gobiernan el tema, a los representantes locales, permitiendo de ese modo ensanchar los campos de acción de éstas, al tiempo que proveer una cierta catalogación por actividad que, aunque muy genérica, resulta útil. Ej. www.rau.edu.uy, donde edu.uy se lo considera uno de los seis dominios de segundo nivel de que dispone el ente regulador uruguayo para manejar las asignaciones según categorías funcionales (los restantes son gub.uy, org.uy, com.uy, net.uy y mil.uy). En el ejemplo que se cita se trata de la "Red Académica Uruguaya", que administra la Universidad de la República, y que en mérito conjunto a su naturaleza y nacionalidad está autorizada a operar bajo el dominio re-catalogado como de segundo nivel edu.uy (siempre la nacionalidad al extremo final de la identificación, ya que la Entidad reguladora local no tiene jurisdicción sobre el dominio primigenio .edu, como no lo tiene ningún país en el actual esquema organizativo de la materia, y sí otras entidades a las que nos referiremos luego).

Otro ejemplo que va más allá del esquema básico presentado, es la inclusión del nombre del proveedor de servicios vinculados con la realización del sitio y/o su conexión a la red. O bien, la denominación de una serie de reparticiones y/o sub-reparticiones de la institución, iniciativa, etc. que se ha puesto en vitrina. Por esta vía, algunos "nombres de dominio" van adquiriendo longitudes considerables: Por ejemplo, sepan Vds. que pueden encontrar interesantes "cuentos de escritores latinoamericanos" en la siguiente dirección: http://www.geocities.com/SoHo-/Café/9980/sc-latinos.htm. Una larga secuencia alfanumérica, las hay mayores por cierto, en la que al menos alcanzamos a distinguir la presencia del conocido "geocities", uno de los más grandes -sino el más- alojadores de páginas web a nivel mundial.

Importante precisar en este punto, que cada nivel se hace responsable por la organización adecuada -en términos identificatorios- del nivel que le sigue hacia abajo (como la pirámide jerárquica que es). Pero también aclaramos que el breve apunte anterior no refiere a la responsabilidad de los alojadores de páginas web por el contenido legal o ilegal de dichas páginas: uno de los temas más debatidos en la actualidad en materia de "derecho de internet". Tan sólo, en esta oportunidad, aludimos a una correcta organización y funcionamiento del sistema, desde el punto de vista técnico (es decir, que los mensajes circulen efectivamente, desde y hacia el lugar que los envía el usuario).

1.2. Organismos rectores

Si bien se acostumbra decir que Internet "no tiene dueño ni gobierno", lo cierto es que organizaciones dotadas de mayor o menor ecuanimidad y representatividad de los intereses en juego (a gusto de quien analice y tome postura sobre el tema), le han venido dando a la red por lo menos la fisonomía técnica que mantiene hasta el presente.

Organizaciones mayormente provenientes de los EE.UU. Hay que decirlo sin ambages, desde que ha sido en este país donde -al fin y al cabo- nació y adquirió cuotas enormes de desarrollo esta tecnología. Una tecnología que pronto alcanzó extensión y uso mundiales, pero que a causa de su vínculo genético continúa llevando en sus entrañas la oscilante contradicción (a veces bien conjugada, a veces no tanto) entre el paternalismo del progenitor y el querer de sus hijos pródigos. Dicho esto último en el sentido de buscar abrirse definitiva y completamente hacia la vocación universal y participativa de todos los pueblos de la tierra, también en su cúpula organizativa (por no decir "directriz"), como fenómeno de alcance mundial que es esta red de redes.

1.2.1. Evolución histórica

Por razones que al comienzo fueron meramente mnemotécnicas, un número creciente de sitios web fue adoptando este tipo de identificador nominativo, por lo general el propio nombre de la persona o institución en la vida real, (ej. universidadxx.edu). No obstante ello, rápidamente -y coincidiendo con la propia evolución funcional de Internet- vendrían a primar otros factores para el mantenimiento y evolución del sistema. Al punto que, lo que había sido al principio un simple instrumento para facilitar el conocimiento recíproco entre relativamente escasos actores de una red, se convertiría luego en poderosa herramienta de marketing, al servicio de empresas y múltiples actores de la actual sociedad globalizada, que se encuentran poderosamente atraídos hacia una necesaria presencia en el mayor escaparate mundial. De paso advertir, la tremenda puja de intereses y posiciones encontradas (fundamentalmente dos

bloques) en el plano de los destinos evolutivos de la red, timoneados mediante un original sistema de participación y acuerdos entre múltiples organizaciones y grupos de interés a escala mundial, donde no intervienen -al menos formalmente- los gobiernos sino personas y entidades interesadas en el desenvolvimiento de esta tecnología por diferentes motivos. Ambito en el que se intentan los mayores consensos posibles, a tono con la filosofía de la red, es decir una comunidad interplanetaria y coparticipativa, donde haya espacio para grandes y pequeños.

Como decíamos, pues, no una sino varias organizaciones, grupos de interés, etc., de diversas extracciones, han sido y son los que se ocupan del complejo y distribuido mundo tecno-gerencial que entraña la organización de esta macro-red. De conformidad con la propia naturaleza pública y mundial de la misma. Y es en este terreno donde han venido librándose algunas batallas políticas que reflejan distintas concepciones filosóficas, pragmáticas y hasta económicas, de lo que es -o debe seguir siendo- Internet.

En este tipo de escenarios es donde nace y se mueve hasta el presente el tema que nos ocupa. El DNS, o Sistema de Nombres de Dominio, se origina allá por la década de los 80 en los EE.UU. Su génesis está unida a algunos científicos pioneros que dieron forma a esta tecnología, tal como funciona hoy en día, y que en algunos casos se convirtieron en mitos vivientes, por su prolongada dedicación y demostrada ética al servicio de los más caros ideales de Internet en toda su extensión. Coordinando desde planos técnicos lo que para ese entonces era todavía una iniciativa al servicio de la comunidad científica y militar del país del norte (Arpanet, devenida con el tiempo Internet). Hombres como Jon Postel de la Universidad del Sur de California (figura señera de este entorno, fallecido recientemente), Paul Mockapetris (verdaderamente el creador del DNS, en colaboración con el antes nombrado), y posteriormente Paul Vixie, desarrollaron este sistema de tipo jerárquico, que funciona como una base de datos independiente pero afectada al sistema de las IP. Es decir, en otras palabras: a cada dirección IP le corresponde un nombre de dominio preciso y único.

Originariamente, el Sistema de Nombres de Dominio involucraba solamente instituciones universitarias y militares, donde el "gajo académico" por así llamarlo fue manejado desde un principio por la NSF (National Science Foundation), entidad académica bajo cuya tutela se creó la primera red educativa a vocación global, la NSFnet, sucesora de la primigenia ARPAnet, y directa precursora de lo que hoy conocemos como Internet.

Pero, como se sabe, estas primigenias redes comenzarían pronto a tener diversificaciones y agrupamientos con otras redes e instituciones. El número de máquinas conectadas creció, y fue necesario que la NSF convocara a concurso para desarrollar ciertos servicios capaces de mejorar sustancialmente la red, los denominados network services managers. El concurso lo ganó la compañía privada Network Solutions, Inc., la desde ese entonces conocida "NSi" (o "NSI" según otras fuentes), que terminó asumiendo por contrato con el gobierno de los EE.UU., la tarea de prestar servicios de proveeduría en la materia (asignación de direcciones IP y DNS), ya sea en forma directa como a través de registros delegados. Todo ello bajo la autoridad de las entidades reguladoras (a la época la IANA). Primeramente lo hizo en forma gratuita, pero a partir de 1996 la NSI queda autorizada a cobrar por la asignación de dominios, y así lo hizo. Con lo cual comenzaron las preocupaciones del resto de la comunidad interplanetaria, frente al riesgo -o realidad- evidentes de entrar a padecer un régimen monopólico.

La expiración definitiva del contrato que vincula a esta compañía con el gobierno estadounidense (varias veces prorrogada), está prevista para setiembre del presente año 2000. Pero entretanto la empresa fue la encargada de ofrecer a la comunidad telemática mundial un sistema habilitante para el funcionamiento en la red, en términos cuasi-monopólicos (al menos hasta 1998). Esto sucedió así por lo que respecta a los gTLDs históricos, o sea el .com, el .org. y el .net., más el TLD nacional .us. Labores para las cuales NSI se asoció con el registrador igualmente norteamericano InterNIC , encargado de delegar en los registros nacionales de los diferentes países algunas competencias (fundamentalmente, la asignación de dominios de segundo o ulterior niveles dentro de los respectivos ccTLDs de cada país).

Pero retrotrayéndonos, todavía, a la época de real apertura de Internet al público (tal cual hoy la conocemos, años 1992-1994) fue en ese mismo período que se creó lo que a la postre sería el DNS en forma operativa. Aparecieron, entonces, los primeros gTLD (generic Top-Level Domain) .com, .net y .org, con el propósito de establecer una primaria clasificación, en favor de organizar el agrupamiento de quienes buscaban usufructuar los servicios que proporcionaba el sistema.

A nivel de organismos rectores, y para toda esta primera época, sería la IANA (Internet Assigned Numbers Authority) la que se ocuparía del tema de asignar los nombres de dominio y las direcciones IP, delegando sus poderes en tres organismos que se repartieron en grandes zonas geográficas dichos poderes: 1) InterNIC (Internet National Information Center), entidad perteneciente al Departamento de Comercio americano, para la zona de los EE.UU, y todas las regiones no cubiertas por las restantes; 2) el RIPENCC (Reseaux IP Européens - Networks Coordination Center) para Europa; y el APNIC (Asia - Pacific Information Center) para la zona de Asia y el Pacífico.

Si bien la IANA no desaparece, a partir de 1998 surge una nueva entidad con roles centrales en la materia, la Internet Corporation for Assigned Names and Numbers (ICANN),organización no lucrativa como la anterior, encargada de las alocaciones de direcciones IP y la gestión del DNS, actividades que hasta ese momento eran llevadas a cabo bajo contrato del gobierno de los EE.UU. por la IANA y otras entidades.

En un período intermedio estuvo actuando también el International Ad Hoc Commitee conocido como el IAHC, una suerte de task force creada a iniciativa de numerosas organizaciones internacionales, entre ellas la OMPI y la ISOC, que se autodisolvió con el dictado, y suscripción por los países, de un documento titulado gTLD-MoU, conteniendo recomendaciones sobre la administración y gestión de los gTLDs.

Es un hecho, pues, que la historia institucional de los "nombres de dominio" en Internet, si bien relativamente corta, se mueve alrededor de esta parafernalia de organismos creados ex-professo algunos de ellos (IANA, IAHC, ICANN...), o bien de existencia anterior pero llamados a co-participar en el esquema regulador por mérito a competencias naturales previas, afines al nuevo fenómeno (OMPI, UIT, y en buena medida la ISOC -Internet Society- dado su alcance más amplio que el restrictivo campo de los nombres de dominio). Contándose, además, las empresas señaladas y otras, sin cuya mención no estaría completo el mapa internacional en esta materia.

Es un hecho, asimismo, que a este cúmulo de entidades (algunas de las cuales se disuelven cumplidos sus objetivos, otras permaneciendo para solaparse temporalmente por razones estratégicas con las nuevas estructuras), se le suma una línea de acciones y sucesos, también de complicado seguimiento. En este punto, las posturas y políticas desenvueltas se develan a través de varios informes y documentos provenientes, ora del gobierno estadounidense (el Libro Verde y el Libro Blanco), ora de organismos llamados a intervenir ad hoc en la materia (el Proceso... de la OMPI; el MoU, un documento básico bajo el cual se busca la reestructura del sistema, respaldado por organizaciones de todo el mundo entre ellas la OMPI y la UIT, y cuya aparición y suscripción por un gran número de países -alrededor de 200- significó la autodisolución de la IAHC).

Todo este voluminoso -y seguramente incompleto- detalle evolutivo, es lo que ha ido pautando un lento y trabajoso proceso de reforma vivido, y que se vive aún hoy. Un período que abarca no más de tres o cuatro años a esta parte. En última instancia se aprecia un denodado esfuerzo por acompasar -no siempre con éxito- el ritmo acelerado e incremental que en muchos órdenes, y en el mismo tiempo, experimentó Internet. Fundamentalmente a partir de que pasa a convertirse en vector de figuración y negocios para las empresas. Dejando entrever, incluso de forma ostensible, la disconformidad de todas las partes involucradas -mayormente el conglobado europeo- en lo que hacía al régimen imperante del DNS, particularmente por dos motivos:

A) La insuficiencia cada vez mayor del sistema para contemplar necesidades de funcionamiento incrementado, siendo una de las puntas más visibles del problema la saturación del dominio .com, y su manejo monopólico por una empresa estadounidense.

B Los roces cada vez más fuertes del sistema de nombres de dominio con el sistema jurídico marcario.

Es así que, sobre todo en este último período, el panorama se ha visto visiblemente dominado por la impronta de intereses encontrados, fundamentalmente entre algunas empresas norteamericanas y hasta el propio gobierno de los EE.UU, de un lado del escenario, con el resto de la comunidad internacional por el otro (léase Europa a nuestros ojos vista, desde el momento que América Latina -por ejemplo- recien comienza a despertar a niveles gubernamentales respecto de la importancia de todo lo que entorna a Internet... y aún no sienta presencia fuerte en este sector crucial de los nombres de dominio).

Sin perjuicio de estas discusiones y puntos encontrados -algunos de ellos expuestos en las propias listas de intercambio de que hace gala democrática Internet sobre esta y otras cuestiones- se han podido establecer algunos avances. Se espera que no se produzca el congelamiento o statu-quo, producto de la dificultad por la que atraviesan las negociaciones sin que hayan decantado totalmente los asuntos en disputa.

1.2.2. Funcionamiento actual de las asignaciones. Reglas.

Sin perjuicio de reformas en ciernes (que se comentarán en el próximo apartado) el panorama actual en materia de asignación de nombres de dominio es el que sigue.

1º) La empresa NSI ya no tiene el monopolio para los dominios de primer nivel .com, .org y .net, a través de InterNIC. La misma sigue actuando a través de sus oficinas asociadas (unas pocas, diseminadas por EE.UU y otras partes del mundo), pero se le han sumado organizaciones competitivas, como el CORE, Internet Council of Registrars (una especie de cámara de registradores asociados, y ella misma registrador, fundada en 1996 a consecuencia de los planes de reestructura emanados de la ISOC y la IANA).

2º) Por lo que refiere a los dominios de primer nivel con base territorial, en su momento la InterNIC delegó en entidades nacionales de cada país -generalmente reparticiones universitarias o entidades ministeriales afines al tema como son los Registros de la Propiedad Intelectual- la asignación de dominios bajo código local. En el caso uruguayo, el NIC local funciona en la órbita de la Universidad de la República, a través de su servicio de cómputos (http://www.rau.edu.uy/rau/dom), que administra los dominios de entes y particulares que deseen abrir un sitio web bajo la extensión .uy, esté o no físicamente radicado dentro de nuestras fronteras (Uruguay es uno de los países que no pone restricciones domiciliarias a quienes ingresen en su dominio). Asimismo, en el caso uruguayo, parte de dicha administración -concretamente la referente al dominio .com- ha sido delegada a la empresa estatal de telecomunicaciones ANTEL www.dns.antel.net.uy. Cada país -entonces- fija reglas particulares al respecto, las que se informan en las páginas webs respectivas. Estas reglas van desde la extensión que deben tener los nombres a registrar, hasta cuestiones vinculadas con posibles conflictos que pudieran suscitarse (en especial con el derecho marcario). Es interesante comparar el nivel de exigencias según los países. Por ejemplo Francia es bastante exigente a la hora de controlar la asignación de un nombre de dominio (ejs. obligación de llenar ciertas fórmulas denominadas "Kbis"; exigencia de certificado de registro de la propiedad industrial para el caso que el nombre a depositar sea una marca, con lo que elimina de raíz no pocos conflictos; más otra serie de resguardos). Otros países, como Uruguay, se limitan a enunciar algunas causas de eliminación a *posteriori* del registro, cuando -por ejemplo- "alguna autoridad competente determine que el dominio en litigio no corresponde al titular actual". Son diferencias, claro está, de nivel de desarrollo en la materia. Para bien o para mal, Uruguay no posee un contencioso judicial sobre el punto, como el que posee Francia, e intenta disminuir con este tipo de reglas administrativas.

3º) Al margen de las reglas administrativas (variables como se dijo antes, según el país u organización que las haga y aplique), la única regla que rige en la materia es la prelación temporal en el registro: *first come, first served, o como decían los romanos prior in tempore potior in iure.* Para el caso, "el que primero inscribe es el que tiene mejor derecho". Esta es la única regla de oro que rige actualmente el sistema mundial en la materia, y que no pocos conflictos está ocasionando -según veremos luego- con materias reguladas y existentes con anterioridad a la aparición del DNS, en especial lo que hace a la Propiedad Industrial y Comercial. Los organismos registradores no exigen -como es el caso de las marcas- una búsqueda de patrones de registro iguales o similares, por parte del candidato a inscribir cierto nombre, lo cual abre una brecha importante para posibles contiendas entre ambos sistemas. Está dentro de las políticas de prevención (elemento sobre el cual el informe OMPI, entre otros, hace especial hincapié en cuanto a necesidad de implementar) que las entidades partícipes del sistema recomienden e incentiven este tipo de búsquedas, de modo previo a resolver la adopción de un determinado un nombre de dominio. De hecho existen servicios en la red apostados a tales efectos (los llamados Whois).

1.2.3. Organización en ciernes

El excesivo peso de los EE.UU. en la coordinación de los destinos de Internet (en detrimento del resto de la comunidad mundial), la situación cuasi monopólica y privatística del principal dominio internacional que es .com en manos de una empresa estadounidense durante largo tiempo, la saturación terminológica de dominios de segundo nivel ubicados en .com así como el desproporcionado volumen alcanzado por éste con respecto a otros dominios genéricos existentes, los conflictos de derecho y jurisdicción, el combate contra prácticas aberrantes (cybersquatting también llamado domain name grabbing, que en español ya se ha traducido por "ciberocupación"). Todos estos factores han incidido para que desde no hace más de tres años a esta parte comenzara a tomar forma una reestructura del régimen de DNS a escala mundial.

A través de una larga serie de consultas globalizadas (procedimiento consolidado para ir pautando los rumbos y evoluciones que sigue toda esta materia, y que aplican varias organizaciones involucradas, entre ellas OMPI), se fue abriendo camino trabajosamente, y como producto de arduas negociaciones que continúan llevándose a cabo aún en el presente, un nuevo esquema organizativo mundial en la materia. Tendiente, justamente, a mejorar los flancos débiles del sistema anterior.

Esta nueva organización, parte de la cual ya está en marcha de un modo que parece irreversible, se articula bajo las siguientes líneas maestras:

A = Un rol preponderante aunque sometido a transiciones (y quizás también a "transacciones") como el que se adjudica a la ICANN. Este organismo está -o estará- compuesto por: un Consejo de Administración de 9 miembros; unos organismos de base destinados a tratar las proposiciones relativas a protocolos IP (el PSO), direcciones IP (el ASO) y nombres de dominio (el DNSO), compuesto este último por 7 grupos de trabajo; unos Comités de Consejo y una Asamblea de miembros que se configura como panel de usuarios del web con varias funciones.

B = La creación de siete nuevos dominios genéricos, clasificados en categorías que vendrán a descongestionar el abarrotado .com, y que son:

.firm para negocios o firmas
.shop para ofrecer bienes o servicios a la venta
.web para entidades o grupos proveedores de servicio a la propia red
.arts. para entidades o grupos dedicados a cultura y entretenimiento
.rec para entidades o grupos de recreación
.info para servicios de información
.nom para personas que buscan registrar sus propios nombres (páginas personales)

Estos nuevos dominios genéricos de primer nivel se suman (no sustituyen) a los anteriores existentes, estando las organizaciones y empresas acreditadas habilitadas desde ahora para efectuar "reservas de asignación" en cuanto a nombres de segundo nivel se refiere. Lo que significa que ya existe un mercado en fase de explotación inicial a tales efectos, que aquéllas organizaciones y empresas vienen sumando a su cartera a cuenta de lo que se lanzará en futuro próximo.

C = Sometimiento de los conflictos entre requerientes de nombres de dominio y terceros que se sientan asistidos de algún derecho violado, a una batería de instancias de arreglos administrativos, mediaciones, arbitrajes, etc., o sea "justicia alternativa". Esto es propiciado y ordenado desde el ICANN, por ejemplo, a través del cuerpo normativo denominado Uniform Domain Dispute Resolution Policy - UDRP. Los poderes y competencias de estos organismos incluyen, mediaciones en línea con costos más reducidos que los tradicionales procedimientos off-line, suspensión del nombre en disputa, su atribución a terceros, examen del certificado de depósito marcario, exclusión de ciertos nombres (ej. marcas notoriamente famosas), etc. La normativa UDRP puede ser consultada en www.icann.org/udrp/udrp/htm .

D = Distinción neta entre la figura administrativa del sistema, que será una entidad sin fines de lucro (el re-

gistry), y aquéllos que se dedican a título comercial a promover este nuevo renglón de negocios como es el ofrecimiento y gestión de un nombre de dominio para quien está necesitando uno. (el registrar).

2. LOS ASPECTOS JURIDICOS

Un sistema de trabajo proveniente de la técnica, por lo general es concebido llevando adelante escrupulosos requerimientos de dicha técnica. Sin embargo, en el curso de ese proceso de creación y evolución, no siempre se cuidan otros flancos o cuestiones muy diferentes pero que igualmente vienen a quedar atrapados cuando el fenómeno es suficientemente vasto. Luego cuando se reacciona... ya es un poco tarde. El problema está arriba de la mesa, por falta de previsiones que podrían haberlo evitado en su momento. Esta es la sensación que a uno le deja, desde una óptica que no es la del técnico, lo que ha sucedido, palabra más o menos, con el Sistema de Nombres de Dominio respecto del sistema jurídico a secas, aunque nada de ello es irreversible, afortunadamente.

Y no todos son problemas, sin embargo. Hay cuestiones que Internet viene favoreciendo, asimismo para el propio avance del Derecho. Otras son, más bien, "arreglos de cuentas" o "transacciones" que debe hacer el mundo de la técnica con el mundo del Derecho, para que todo funcione lo mejor posible, en pos -como mínimo- de no avasallar derechos ya consolidados, tanto de particulares, como de instituciones y de la sociedad en su conjunto.

2.1. Algunas cuestiones desde donde arranca la problemática jurídica

Hay que comenzar por explicar, con carácter previo, algunas cuestiones que están en la base misma de los problemas jurídicos aparecidos con relación a las prácticas de inscripción de los nombres de dominio.

Para comenzar -y esto es reedición de algo que ya expresamos antes- resulta inconcuso que todo este asunto de los nombres de dominio adquiere relevancia para el Derecho, a partir de la utilización cada vez más ostensible de Internet por parte de las empresas y corporaciones. Una utilización a efectos tanto de ganar presencia en la red (vector de publicidad) como de implementar canales paralelos o novedosos para sus propias actividades, muchas de las cuales pueden llevarse a cabo -con mayor o menor grado- por vía cibernética (fundamentalmente el comercio electrónico, en su variada gama).

Luego hay que tener conciencia de que no existen diferencias técnicas de principio en cuanto al alcance de un dominio genérico nacional (ej. .uy) y uno genérico internacional (ej. .com). Ambos son consultables desde cualquier parte del globo. Pero asimismo hay que saber que el poder de difusión de ambos vectores es absolutamente desparejo. El country code lo utilizan entidades -hablemos ya de empresas- que buscan una presencia local. El top level, en cambio apunta (en términos identificatorios o evocativos de la eventual clientela que ingresa al sitio), hacia un mercado ampliado y extendido tanto dentro como fuera de fronteras. Si a ésto lo complementamos con el trabajo que hacen los grandes y más utilizados "robots de búsqueda" en Internet, en cuanto a que priorizan el .com en sus estrategias de barrido para recuperar información puntual solicitada por los usuarios y alojada en sitios desconocidos de antemano, tenemos que las diferencias y consecuencias en uno y otro caso son palpables. De ahí la preferencia por adscribir al dominio genérico .com, lo que ha llevado a su saturación. Y de ahí también el aprovechamiento ilícito de esta situación que han hecho algunos inescrupulosos en la red, dando origen a una práctica condenable denominada "ciberocupación", de la que trataremos luego.

2.2 Derecho marcario y nombres de dominio. Principios y casos

Existen dos aspectos fundamentales que separan el régimen de nombres de dominio del régimen jurídico marcario.

Por un lado, en Derecho marcario rige el principio de especialidad, en tanto los depósitos de marca están organizados por clases de productos y servicios. Es así que un signo es generalmente registrado como marca en una o pocas clases pertinentes dejando liberado un amplio elenco de categorías, lo que permite que ese mismo signo sea utilizado por terceros en relación con otras clases diferentes de actividad. Esto es una gran cosa, que favorece la

práctica económica. Pero lamentablemente esta regla no encuentra equivalente dentro del sistema de nombres de dominio, donde una vez ocupado el dominio de primer nivel con determinado nombre, queda vedada la utilización de ese nombre, al menos dentro de ese mismo nivel. La extrema generalidad de los dominios genéricos funcionales actualmente vigentes, así como el aspecto reduccionista que supone el tener que optar por inscribir en los dominios nacionales como única alternativa frente a la ocupación previa del dominio internacional, eximen de comentarios acerca de las desventajas del sistema tal cual fue concebido.

La otra diferencia entre ambos regímenes, que está incidiendo fuertemente en la explicación y génesis de muchos de los conflictos que se presentan, es el alcance jurisdiccional de ambos sistemas. El DNS en tanto sistema regulador es de alcance mundial. Internet no conoce fronteras por definición, y un nombre de dominio tiene los mismos atributos desde un punto de vista regulatorio, tanto esté ubicado en un primer nivel de tipo genérico-funcional como geográfico. Al contrario de ello, las legislaciones marcarias están fuertemente basadas en el principio de territorialidad, lo que determina la existencia exclusiva de depósitos nacionales o -a lo sumo- regionales (no hace mucho que se está abriendo camino esta última noción, en relación proporcional al auge del Derecho de la Integración en los últimos años), y la intervención de una legislación y judicatura locales.

Los problemas que se han venido presentando entre el sistema ND y derechos afines a la materia (especialmente el derecho marcario), son de especie diversa.

Es evidente que la reproducción no autorizada como nombre de dominio de una marca legítima y vigente, perteneciente a un tercero, resulta violatoria del derecho marcario. Pero una brevísima clasificación se impone, pudiéndose apelar a la tipología que a continuación exponemos.

2.2.1. Simple contradicción entre ambos sistemas, por sus alcances naturales y sin que haya necesariamente una actitud dolosa de las partes involucradas

Es el caso de una empresa X que, siendo titular de una marca determinada, no la ha inscripto como nombre de dominio. Luego arriba la empresa Z e inscribe el mismo (o similar) término como nombre de dominio dedicándose a una clase de actividades diferente de aquélla a la que se dedica la primera. En principio lo puede hacer, atento a la ausencia del principio de especialidad en el sistema de nombres de dominio (salvo que se trate de una "marca notoria" en cuyo caso la balanza gira a favor del titular marcario). Y como el riesgo de confusión entre ambos nombres es inexistente -por tratarse de empresas operantes en clases diferentes de actividad- es justo que se ampare a quien inscribió dicho término como nombre de dominio (aplicación de la regla "first come, first served"). Ejemplo de este tipo de contenciosos: affaire Alice francés, donde los tribunales terminaron por sostener que a la poco previsora empresa X le quedan los recursos de acudir a los dominios .com o bien .tr.fr (esto último como particularidad que algunos países como Francia utilizan, que autoriza este tipo de extensiones cuando el nombre de dominio postulado es una marca registrada -trade mark-.).

2.2.2 El "cybersquatting" o "domain name grabbing" o "ciberocupación"

Son los casos más notorios, los que han adquirido difusión en los grandes medios de difusión. La conducta es simple, no obstante su enorme poder agresivo. Una empresa tradicional y bastante conocida, con su denominación social impuesta en el mercado y sus marcas -hasta puede que famosas- debidamente inscriptas, decide subir sus nomenclaturas a las vitrinas cada vez más irresistibles de Internet. Pero al intentarlo se ve bloqueada porque un tercero, por lo general oscuro y desconocido, a veces domiciliado en otra parte del planeta, ha registrado esos mismos nombres en fecha anterior.

El impacto puede ser tremendo. A partir del mismo momento en que los dominios empezaron a verse como marcas (transición hacia el sentido mercantil de la red), surgieron los piratas. Se dice que un asesor jurídico comenzó a participar de la política organizativa de Internet, cuando su mejor cliente, la cadena de comidas rápidas McDonalds, fue objeto de una maniobra de este tipo. Afortunadamente, parece ser que en este caso la inscripción del nombre con carácter previo la hizo un periodista especializado en el tema, con el único propósito de dar un alerta acerca de la viabilidad y alza de este tipo de acciones, solicitando y recibiendo a cambio una módica suma que

donó a una institución educativa. Pero otros damnificados no corrieron igual suerte: o se plegaron a planteos extorsivos o acudieron a los tribunales.

En la mayoría de estos casos, comprobado que fue el fraude a través de ciertos elementos de convicción (no utilización del sitio, antecedentes desconocidos del infractor en el campo de actividad al que apela la marca o nombre en cuestión, preeminencia del derecho sobre la "denominación social" por sobre el régimen de nombres de dominio...), los tribunales han dado la razón a las víctimas.

Siempre dentro de esta modalidad de fraudes, algunas estratagemas más complejas que el tipo relatado han recibido igualmente condena judicial. Por ejemplo la hipótesis del affaire SFR vs. W3 Systems Inc, donde la segunda desarrollaba una actividad comercial de venta de nombres de dominio por Internet, previa inscripción de más de 300 nombres mayoritariamente coincidentes con notorias marcas francesas. Para acentuar la presión de compra de estos nombres sobre los verdaderos titulares de tales marcas, el pirata puso en movimiento algunos sitios con dichos nombres, redireccionando el tráfico de consulta hacia terceras empresas de igual ramo, vale decir la competencia. Se trató, pues, de un caso de "ciberocupación" al que se agregó la noción de "parasitismo", que viene del derecho informático y la propiedad intelectual clásicos, e ingresa desde múltiples ángulos al nuevo derecho de internet. El caso fue castigado por los jueces con ejemplar severidad, con una sanción sin precedentes de un 1 millón de francos en concepto de daños y perjuicios.

Estas situaciones de "desvío de tráfico" en la red son bastante frecuentes. A veces justificadas (ej. cambio de dirección de cierta página), pero otras realizada con propósito fraudulento (parasitismo) por sujetos que poseen altos conocimientos técnicos. Por estos senderos criminosos se llega, por ejemplo, a ubicar en el código fuente de un sitio web la marca de la competencia. La misma permanece oculta en general, pero cada vez que se efectúan búsquedas que involucra de una manera u otra a la marca legalmente constituida, a través de los poderosos browsers existentes, el sitio del falsificador será levantado entre las primeras respuestas. Y la dificultad está en que son muchas las estrategias a prevenir y despejar, como modo de contrarrestar estas prácticas.

En materia de "marcas famosas", por otra parte, existen varios pronunciamientos a favor de la protección de tales, cuando son objeto de intentos de registro como nombres de dominio a los efectos de su posterior monetización. Se estima que es un acto de falsificación y dilución del carácter distintivo de la marca, que intenta indebidamente sacar provecho de la reputación de la marca a favor de terceros (ej. desvío de clientela), o bien preparar el terreno para una operación extorsiva no siempre condenable en la esfera penal -de lo contrario no sería tan abundante- atento a las fisuras que presenta el sistema de protección jurídica en la materia.

2.2.3. Falsificaciones directas o clásicas, más o menos desembozadas

Existen aproximadamente 250 extensiones de dominios genéricos, contando los geográficos y los funcionales. Es imposible, de tal forma, que los propietarios legítimos de marcas hagan depósito paralelo de las mismas en todos y cada uno de los niveles habilitados para nombres de dominio. Del mismo modo que no depositan tales marcas en todos y cada uno de los registros marcarios del planeta, ni en todas y cada una de las clases dentro de un mismo país. Con una diferencia no despreciable en uno y otro caso: el alcance nacional y mundial, respectivamente, de ambas situaciones.

Como todos sabemos, existen hoy en día los llamados "paraísos", en tanto países donde las legislaciones de determinadas materias son extremadamente blandas o inexistentes, con el único propósito de atraer inversores (cuando no... malhechores). Referido ésto al tema que nos ocupa, ya se observa la existencia de este tipo de países -que incluso están en una conocida "lista especial"- donde es posible registrar nombres de dominio sin mayores exigencias.

Sin necesidad de acudir a estos paraísos, si cupiera la expresión alegales (por similitud con "amorales"), los jueces de diversos países han estado bastante unánimes en condenar este tipo de falsificaciones clásicas, es decir cuando el depositario del nombre coincidente (o similar) de la marca no tiene ningún tipo de autorización de ésta a tales efectos, aún a falta de propósitos decididamente extorsivos. Así en Alemania, donde se condenó por falsifica-

ción de marca y concurrencia desleal a quien registrara "epson.de" sin demostrar vínculo alguno con la conocida firma. También en Alemania, por otro caso similar donde se había registrado el dominio "toyota.de".

Igualmente en Alemania se dio un caso de instrumentación procesal particular: una actio in rem, es decir contra los nombres de dominio en si mismos. Se trató del conocido constructor de automóviles Porsche que, ante el registro por parte de falsificadores de su nombre sobre más de ciento treinta extensiones diferentes, debió acudir a este mecanismo por la imposibilidad de ubicar a todos los depositarios. En nuestra referencia del asunto no existía resolución todavía en la contienda así entablada.

En Gran Bretaña, donde ha habido varios casos tanto de "ciberocupación" como de "falsificaciones clásicas" que llegaron a tribunales, y donde incluso se llevó ante los tribunales a empresas vinculadas con la prestación de servicios para la red (Harrod´s Ltd. Vs. UK Network Services). En Italia hubo decisiones ya en similar sentido, como es el caso Amadeus Marketing Italia c/ Lógica.

2.2.4. Otros casos de falsificaciones marcarias en internet

No son asuntos vinculados a los nombres de dominio, pero sí a vicisitudes que ha provocado Internet en el derecho marcario. Se han verificado falsificaciones de conocidas marcas con apoyo y actuación de la red. Así el affaire L´Oreal en Francia, referido a la venta telemática de la línea de productos de esta empresa apropiándose fraudulentamente de su marca.

2.3. Los problemas de jurisdicción y la "ciberjusticia"

El problema de la jurisdicción competente en materia de contiendas relacionadas con Internet, es un punto trascendental y concreto sobre el cual se viene ocupando la jurisprudencia y doctrina en la materia. Para el caso imaginemos una empresa X que es titular de una marca dentro de cierto país, en tanto la empresa Z luego pone en funcionamiento en otro país un sitio web bajo la misma denominación, y tiene asimismo la marca registrada en su propio país, diverso que el de la empresa X. Agreguemos para el caso que se trata de la misma clase de actividades, y hasta productos idénticos.

Al no existir una justicia internacional que se ocupe de esta temática, y dado el carácter extraterritorial de Internet, es evidente que este tipo de casos -como otros que ocurren en torno a otras cuestiones de la red- presenta el desafío jurídico de buscar el juez competente. Para la hipótesis planteada, no caben dudas que los jueces radicados en el país de la empresa X resultan totalmente competentes como para entender en un juicio de ésta contra la empresa Z. Esto es así por cuanto la emisión por Internet desde un cierto país afecta el resto de la comunidad de países, entre ellos el punto de conexión dado por la radicación de la empresa afectada. Otra cosa es opinar acerca de la mejor solución jurídica para resolver el fondo de la cuestión planteada. Véase que no se trata de "derechos de autor" lo que está en juego (de alcance mundial), sino de especies marcarias (por definición de alcance nacional), contra un nombre de dominio depositado en fecha anterior.

¿Cómo juzgar la reproducción por Internet de un término, en tanto es objeto de derechos privativos vigentes en dos estados?. Es un menudo problema. En el affaire Payline los jueces franceses optaron por dar la razón al demandante francés (empresa X para seguir con el ejemplo), en contra del demandado alemán (empresa Z). Pero la solución es sumamente discutible. Si se le hubiera recurrido demandar primero en fecha a la empresa Z en lugar de la empresa X -incluso ante los tribunales franceses, Tratado de la Unión Europea mediante- seguramente habría salido triunfante, porque su derecho también es protegible. Entonces, se cae en la inseguridad jurídica de consagrar el derecho a favor del primero que accione ante la Justicia.

Dado este y otros tipos de dificultades, es que se ha venido imponiendo en la red el concepto de "ciberjusticia". Teniendo en cuenta costos y tiempos que insume un proceso jurisdiccional estatal, no son pocas las ofertas destinadas a resolver conflictos -particularmente los nacidos en la propia red- a través de mediaciones y arbitrajes llevados a cabo en línea. Las directivas más recientes del ICANN, favorecen este proceso al prever la aplicación de estas instancias arbitrales a través de tribunales "en línea" para conflictos vinculados a "nombres de dominio". (ver infra 1.2.3. "C").

No es del caso extendernos en esta oportunidad acerca de los "cibertribunales" y el "magistrado virtual", uno de cuyos ejemplos hemos podido advertir que existe en Perú, al que se llega por http://www.cibertribunalperuano.org . En cambio haremos una breve comentario acerca del Centro de Mediación y de Arbitraje de la OMPI, por involucrar directamente el tema de la ponencia.

Este Centro fue creado en 1994 en el seno del Bureau Internacional de la Organización, y se trata de un organismo que -como cualquier otro cibertribunal- apunta a resolver los conflictos en línea. Actúa desde 1998, ya sea por la vía de la mediación como del arbitraje. Su intervención debe estar expresamente prevista en la relación contractual que vincula a las partes, y a tales efectos el propio Centro propone determinados textos de redacción de tales cláusulas. El procedimiento se desarrolla conforme las reglas del propio organismo, que se relacionan con cuestiones atinentes a la confidencialidad de la actuación, sus costos, imparcialidad e independencia, ley aplicable, etc.

La intervención particular de este Centro en cuestiones vinculadas a los nombres de dominio surge y se aplica a partir del gTLDMoU, concerniendo -como es obvio- a los nombres de segundo nivel registrados en dominios genéricos de primer nivel alcanzados por dicho Memorándum.

3. BREVISIMA REFERENCIA DEL TEMA EN IBEROAMERICA

Desde el punto de vista político-técnico, los países tienen sus NICs locales al igual que el resto del mundo, denominación que significa Network Information Center´s. En España se esta dando una discusión en estos momentos acerca del espacio institucional más adecuado para instalar este nodo, y hemos asistido a una polémica en la web con duras críticas al sistema actual.

Sin perjuicio de estas unidades nacionales, se observan esfuerzos también por dar solvencia y fuerza a ciertos movimientos integradores regionales, como es el caso de Latinomérica. A este respecto la LACNIC, funciona como una organización non profit (como muchas otras creadas para manejar este tipo de instancias relacionadas a Internet) para el Registro Regional de Direcciones IP, Números de Sistemas Autónomos, resolución inversa y otros recursos para la región latinamericana y caribeña. Integrada y/o apoyada por otras entidades regionales vinculadas al uso y explotación de las redes de telecomunicación (ENRED, ECOMLAC...), esta novel entidad se perfila como el interlocutor oficial de la materia frente al ICANN para nuestra región. Pueden verse más detalles en su sitio www-.lacnic.org

En lo que refiere al plano contencioso, la región ha debutado ya -aunque en escala menor que otras regiones, con algunos conflictos que llegaron hasta los tribunales. En España están los casos OZU, SERTEL, NOCILLA, NEXUS y UNI2; en Méjico el caso NESTLE; en Brasil el caso AOL; y en Argentina el caso FREDDO. Excuso el comentario de ellos en homenaje a la brevedad de la ponencia, y remito a la excelente recopilación y comentarios -no sólo de la región sino también del resto del mundo- existente en el único sitio informativo especializado de habla española, que opera bajo la dirección de Javier Maestre: www.dominiuris.com

4. REFLEXIONES FINALES

La comunidad internacional parece estar queriendo re-edificar los viejos paradigmas de entendimiento y colaboración entre los seres humanos de todo el planeta, alrededor del espacio de necesidades técnico-gerenciales de una herramienta tan poderosa y extendida como es la red mundial Internet.

Se vienen realizando esfuerzos enormes en este renglón de actividades, orientados en esa dirección. Las circunstancias lo requieren por la complejidad, importancia y vastedad de intereses entrelazados. Lógicamente se trata de intereses muchas veces encontrados, que aún así -en no pocos casos- admiten consideración y respeto. Tampoco es poca la expectativa reformista. Será cuestión, pues, de lograr consensos, en beneficio de algo que concierne a uno de los puntos neurálgicos de la red actualmente. Un asunto del cual depende en gran medida el ritmo y dirección que tomará Internet en los próximos años.

En la óptica particular que atañe al Derecho, es realmente buena opción que haya tomado cartas en el tema la OMPI, promoviendo profundos procesos de discusión, y librando recomendaciones a ser aplicadas por los organismos directamente competentes en la ejecución técnica y gerencial de estas estructuras. Vemos, pues, como muy conveniente preservar y renovar estos viejos pero necesarios pilares de la Propiedad Intelectual, tan caros al Derecho y tan en contra de aquéllos que piensan que en Internet vale todo. Sin perjuicio de todas las reformulaciones que sean necesarias (¿acaso el Derecho no tiene entre sus postulados básicos también la libertad, que tanto se defiende en Internet?).

La Propiedad Intelectual debe, sin embargo, integrar, o por lo menos considerar, los aspectos conflictivos que la enfrentan a estas nuevos elementos que son los "nombres de dominio", producto de la necesidad de organizar adecuadamente la cada vez más compleja sociedad de la información. Como sostiene la propia OMPI en la pág. 4 de su extenso Informe Final ("Proceso..."), se trata de asegurar "el funcionamiento ordenado del mercado, evitando confusión y engaño... función principal de las marcas, derechos sobre indicaciones geográficas y protección contra la competencia desleal". Y está visto que dicho funcionamiento se ha visto rozado y hasta violentado por un sistema de nombres de dominio que pudo ser justificado en su hora, pero que el descomunal avance de la red lo ha dejado en la retaguardia.

Como se expresa en esa misma página, "la propiedad intelectual se ha convertido en un elemento central de la política económica y cultural del mundo en el que el origen de la riqueza es cada vez más intelectual, en oposición al físico, y en el que los mercados se distribuyen en todo el mundo".

También la misma Propiedad Intelectual debe renovarse a si misma, y lo está haciendo. Por ejemplo con el dictado y suscripción por los países del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC), que viene a actualizar y afirmar en sus aspectos esenciales los Tratados de la Unión.

Pero, y retomamos la cita del mismo informe en la misma pág. 4, "la disciplina de la propiedad intelectual se interesa no solamente por el establecimiento de derechos, sino también por la definición del alcance adecuado de dichos derechos y su relación con otros sectores de la política pública". Es el caso, justamente, de los aspectos promovidos por OMPI en la materia que nos ocupa, los nombres de dominio en Internet. Se trata, como se dice en los medios especializados sobre el tema, de encontrar la interfaz adecuada entre un sistema y otro.

Es por todo ello absolutamente necesario la presencia e intervención del jurista en esta materia. Participando en todas las instancias donde el tema toma vigencia y niveles resolutivos. Y no solamente por aspectos vinculados a la propiedad intelectual, como son aquéllos bajo los cuales hemos centrado el análisis en esta ponencia. No debe olvidarse, entre otros, la posible afectación de los derechos de la personalidad (utilización de patronímicos ajenos), del decoro y las buenas costumbres (nombres ofensivos), entre otra pléyade de asuntos jurídicos que convoca este singular asunto proveniente de la organización técnica de Internet. En eso vienen pujando no solamente la OMPI sino varias organizaciones y personas a lo largo y ancho del mundo.

Finalmente, debe preocupar e interesar vivamente en este dinámico esquema evolutivo, el papel y posibilidades de incidencia que pueda hacer valer América Latina actuando como bloque en las instancias donde se juegan las resoluciones fundamentales de este tópico, frente a otros espacios regionales del planeta que también lo hacen. En este como en tantos otros asuntos de la sociedad globalizada, las cosas se dinamizan y defienden a través de bloques regionales. América Latina ha dado algunos pasos de concentración de esfuerzos, y todo parece estar ir por la buena senda, a través de las acciones que encaran organizaciones como la citada LACNIC. En el futuro inmediato habrá que profundizar en este tipo de direcciones. Con decidida fuerza y conocimiento de causa, con el apoyo de todas las competencias e intereses con que contamos en esta región. Para que el resto de la comunidad interplanetaria nos oiga como es debido. Ya que el desarrollo y avance de Internet no es asunto exclusivamente de empresas. Es un asunto de empresas, pero además es un asunto de alta política de los estados y regiones, sea que intervengan directamente las autoridades de gobierno (EE.UU, Francia, la Unión Europea hacen gala, por ejemplo, -y lo hacen bien- con pronunciamientos específicos al máximo nivel), o también a través de una apertura de cauces y estímulos adecuados para que sean las fuerzas vivas de la sociedad las que enroquen y apliquen a defender esta bandera.

Excursus informationis:

Con excepción de unos pocos materiales consultados off-line (colección D.A.T. de Argentina y Cahiers Lamy Droit de l´Informatique de Francia) nuestra pesquisa ha transcurrido fundamentalmente "en línea". Existe abundante material sobre la temática en la red.

Sobre los aspectos técnicos y políticos, si se quiere una visión completa y actualizada del intrincado proceso que se ha vivido y vive en la materia, no existe camino más seguro que ingresar en los webs y documentos oficiales. Esto es como decir en las entidades internacionales que se han venido ocupando del asunto (entre otras OMPI www.wipo.org, IANA www.iana.org/iana ICANN www.icann.org, ISOC www.isoc.org). Una lista bastante completa de las direcciones web de este tipo de sitios (excluye los latinos) se encuentra en www.corenic.org . La mayor parte de la información proveniente de este tipo de organismos está en idioma inglés, sin módulos paralelos en español. Salvedad expresa, y de destaque, para la OMPI, que mantiene con fineza y total completitud uno de los pocos sitios de esta naturaleza donde pudimos reencontrarnos con nuestra propia lengua.

En cuanto a los aspectos jurídicos no ocultamos nuestra preferencia por lo que ofrecen los sitios jurídicos de internet de ambiente francófono (Francia, Bélgica y Quebec). Sin perjuicio, claro está, de aportaciones puntuales presentes en el ambiente hispanohablante, donde su más lograda muestra la constituye -sin duda- el sitio que orienta Javier Maestre, un especialista de la materia, en cuyo www.dominiuris.com reúne un nutrido conjunto de materiales específicos (casos, doctrina, explicación para novatos, documentos como el muy recomendable Overview of the DNS Controversy de Craig Simon, etc.). Una lista de casos jurisprudenciales norteamericanos, que aparece como exhaustiva, puede ser consultada en The John Marshall Law School de Chicago http://www.jmls.edu/cyber/cases/domain.html , que puede ser accesada también desde el sitio de Javier Maestre.

En muchos artículos de tipo jurídico se incluyen -por añadidura- relatos sobre aspectos técnicos y políticos de la materia. Son también de provecho, con el riesgo, claro está, de no permitir cerciorarnos sobre si estamos ante una información completa y vigente, dado el alto grado de dinamismo y complejidad que poseen estas estructuras. También va aquí el agradecimiento a Erik Iriarte, tanto por los artículos de enorme valía que viene publicando en la R.E.D.I. en toda la amplia gama más actual del derecho de las tecnologías informacionales, provenientes de las más diversas fuentes (y que incluye la temática en examen), como por las noticias puntuales de Derecho y NTI que nos hace llegar diariamente a través de la lista "alfa-redi". En ambos casos hemos encontrado referentes imprescindibles para el conocimiento y seguimiento en forma de este tema tan crucial como es el de los nombres de dominio en Internet.

En cuanto a documentos puntuales que abordan el tema, la que sigue es una lista siempre ampliable, proveniente de diversas fuentes de consulta.

Albertini, Lorenzo - Brevi osservazioni su una delle prime applicazioni ad internet della normativa sui segni distintivi, en http://www.jei.it/informatica_giuridica/online/albertini.htm

Barbry, Eric - Le droit des marques A l´EPREUVE DE l´Internet, en http://www.grolier.fr/cyberlexnet/COM/A980216.htm

Bardales Mendoza, Enrique - Conflicto entre los nombres de dominio en Internet y los Derechos de Marcas, en R.E.D.I. Nº 1 http://publicaciones.derecho.org/redi/N@umero_01_-_Agosto_de_1998/bardales

Bettinger, Torsten - La batalla de los nombres de dominio, en D.A.T. Nº 112/113 (dic.97/ene.98). Buenos Aires.

Cahen, Murielle - Les noms de domaine en .net, .org, .com par rapport au droit français, en http://www.juriscom.net/espace2/mcp4.htm

Cocchi, Laura - Internet e il diritto d´autore: panorama normativo nazionale ed internazionale, en http://www.netjus.org/numero4/cocchi42.htm

Consejo de Estado Francés - Informe sobre la materia (capítulo V: Noms de domaine et droit de marques)

Costes, Lionel - Quel cadre juridique pour l´Internet? en Lamy Droit de l´Informatique, Suppl. Bull. d´actualité Nº 98, diciembre 1997.

Cruquenaire, Alexandre - La problématique des noms de domaine sur Internet, en http://ww.droit-technologie.org/5_2.asp

Chassigneux, Cynthia - Nouvelles voies offertes pour la résolution des conflits en ligne, en http://www.lex-

electronica.org/articles/v5-1/chasifr.htm

Glaize, Fréderic y Nappey, Alexandre - Le régime juridique du nom de domaine en question, en http://www-.juriscom.net/espace2/2/ndm0219.htm

Kaplun, Yasmine - Marques et noms de domaines, en http://www.grolier.fr/cyberlexnet/COM/A971205.htm

Kaufman, Ian Jay - El Sistema de Nombres de Dominio: Actuar ahora o lamentar después, en R.E.D.I. Nº 15 http://publicaciones.derecho.org/redi/N@umero_15_-_Octubre_de_1999/3

Ley de Marcas uruguaya (ley Nº 17.011 del 25-09-98, publicada en D.O. Nº 25.128 del 07-10-98) y Decreto reglamentario Nº 34/999

Maestre, Javier - Comentario al Auto del Juzgado de Primera Instancia Nº 5 de Oviedo de Fecha 2 de Junio 1999, en R.E.D.I. http://publicaciones.derecho.org/redi/N@umero_12_-_Julio_de_1999/maestre

Maestre, Javier A. - Planteamiento de la Problemática Jurídica de los Nombres de Dominio. Comentario a la Sentencia dictada en el caso "Panavisión", en R.E.D.I. Nº 2 http://publicaciones.derecho.org/redi/N@umero_02_-_Septiembre_de_1998/maestre

Maestre, Javier A. - Reflexiones en torno al carácter público e internacional del sistema de nombres de dominio, en R.E.D.I. Nº 8 http://publicaciones.derecho.org/redi/N@umero_08_-_Marzo_de_1999/maestre

Ménard, Bruno - Canada et Etats Unis: Noms de domaine, gestion. Politique de l´ICANN aux Etats Unis. Transfert de gestion vers l´ACEI au Canada, en http://www.juriscom.net/droit/elaw/e-law13-14.htm

Monteiro, José - Contrefaçon et autres atteintes aux marques sur Internet, en Lamy Droit de l´Informatique, Suppl. Bull. d´actualité Nº 98, diciembre 1997.

Monti, Andrea - Domain grabbing, le prime soluzioni, en http://www.interlex.com/regole/amonti23.htm

Monti, Andrea - Prime indicazioni sulla natura giuridica del nome di dominio, en http://interlex.com/regole/a%5fmonti9.htm

Monti, Andrea - The Italian Approach To Domain Grabbing, en http://www.ljx.com/newsletters/

Moyse, Pierre-Emmanuel - Les noms de domaine: un pavé dans la marque, en http://www.droit.umontreal-.ca/faculte/cees/doc/moyse_01.html

OMPI - Informe Final sobre el Proceso relativo a los nombres de Dominio de Internet (versión en español), en http://wipo2.wipo.int

Ortecho, José Manuel - Dominios Internet. ¿Qué son?, en R.E.D.I. Nº 3 http://www.publicaciones.derecho.org.redi/N@umero_03_-_Octubre_de_1998/ortecho

Peyron, Luca - Nomi a dominio-domain name-e propietà industriale: un tentativo di conciliazione, en http://www.gelso.unitn.it/card-adm/Obiter_Dictum/lucapey.html

Plaza Penadés, Javier - La protección de los nombres de dominio en Internet: El informe final de la OMPI y la necesidad de una normativa adecuada, en R.E.D.I. Nº 18 http://publicaciones.derecho.org/redi/N@umero_18_-_Enero_del_2000/10

Robles, Oscar - Cronología del DNS, Nº 8-Boletín de los Nombres de Dominio (1 de septiembre de 19998) www.dominiuris.com

Rolin, Laetitia - Les noms de domaine, en http://www.droit.fundp.ac.be/crid/Enlist/nomsdomaine.htm

SeCIU - Dominio .uy, en http://rau.edu.uy/rau/dom/

Sol Muntañola, Mario A. - Internet: conflictos identificatorios. Las colisiones entre el "DNS" (domain name system) y el derecho de marcas, en http://www.soltmuntanola.com/textos/información3a.html

Solá, Javier - Historia política de Internet, en http://www.aui.es

Verbiest, Thibault - Internet et les noms de domaine. Le rapport de l´OMPI, en http://grolier.fr./cyberlexnet-/COM/A990418.htm

Wery, Ettienne - Domain Name grabbing: La Belgique entre enfin dans le rang, en http://www.droit-technologie.org/5_1.asp

Ziccardi, Giovanni - La tutela giuridica del nome di dominio, en http://www.netujus.org/bulletinita/zic11.htm

REFERENCIAS VITALES DEL AUTOR DE LA PONENCIA:

Nacionalidad uruguaya. Abogado. Doctor en Derecho y Ciencias Sociales. Profesor de Informática Jurídica en la Universidad de la República de su país. Director del Centro de Investigaciones en Informática Jurídica en la misma Universidad (CINADE). Secretario del Comité Organizador del VI Congreso Iberoamericano de Derecho e Informática (Montevideo, Mayo 1998). DEA en Informatica Jurídica y Derecho de la Informática de la Universidad de Montpellier I.

Tema 3

NUEVOS ENFOQUES DE LA INFORMATICA JURIDICA Y DE LOS SISTEMAS APLICADOS AL DERECHO EN EL NUEVO MILENIO

El Sistema Costarricense de Información Jurídica

Licda. Carmen Quesada Chacón / MS. Christian Hess Araya (Costa Rica)

TÓPICO: Nuevos enfoques de la informática jurídica y de los sistemas aplicados al derecho en el nuevo milenio.

SUBTÓPICO: Informática jurídica documental: base de datos.

RESUMEN:

Este documento describe los antecedentes, objetivos y componentes del proyecto "Sistema Costarricense de Información Jurídica" (SCIJ), que pretende posibilitar un acceso integrado a la legislación y jurisprudencia a través de Internet e intranet.

INTRODUCCION

Durante siglos, el almacenamiento y manipulación de la información jurídica en Costa Rica (y probablemente en la mayoría, si no todos los países de la región) se ha efectuado por mecanismos rudimentarios y de poca eficiencia. El soporte fundamental de esa información ha sido el papel, con todas las ventajas –pero, sobre todo, las desventajas– que ello representa.

En el caso de la normativa vigente, la única clasificación y sistematización que existió hasta no hace mucho tiempo en nuestro país (y que aun hoy retiene cierta vigencia) es la de los números de la Colección de Leyes y Decretos. Dicha colección no es más que un compendio cronológico de normas, cuya sistematización no va más allá en realidad del índice que acompaña a cada número. No es sino hasta la creación del "Sistema Nacional de Legislación Vigente" (SINALEVI) en la Procuraduría General de la República que se procura introducir mecanismos tecnológicos para administrar esta labor.

Con respecto a la jurisprudencia, existió también la publicación de colecciones de sentencias de los tribunales superiores, con poca o ninguna sistematización y caracterizándose por un creciente atraso. La introducción del sistema denominado "Master Lex", seguido por algunas otras aplicaciones similares, representa el primer intento de aplicar tecnología en este campo.

Por su parte, cada abogado y cada oficina jurídica pública ha venido manejando, en la práctica, sus propias "bases de datos" –si se nos permite el empleo en sentido amplio de ese término– de información jurídica: tarjeteros, carpetas de leyes y decretos, etc. Mecanismos de clasificación rudimentarios y poco confiables todos ellos, que difícilmente garantizan que los datos estén actualizados y sea confiables.

El Sistema Costarricense de Información Jurídica (en adelante "SCIJ") representa el mayor esfuerzo desarrollado hasta la fecha para la superación de esta problemática.

Este trabajo describe los antecedentes del proyecto, sus objetivos y componentes principales, procurando poner de relieve el carácter verdaderamente revolucionario que posee para los operadores jurídicos del país.

ANTECEDENTES

El artículo 13 de la Ley de la Jurisdicción Constitucional de Costa Rica (1989) estableció –por vez primera en nuestro ordenamiento– el carácter vinculante erga omnes de la jurisprudencia emanada de la Sala de esa materia. La Ley Orgánica del Poder Judicial, número 7333 de 5 de mayo de 1993, establece por su parte en el artículo 5:

"Los principios generales del Derecho y la jurisprudencia servirán para interpretar, integrar y delimitar el campo de aplicación del ordenamiento escrito y tendrán el rango de la norma que interpreten, integren o delimiten. Cuando se trate de suplir la ausencia y no la insuficiencia de las disposiciones que regulen una materia, dichas fuentes tendrán rango de ley."

Con base en lo anterior se refuerza el papel que desempeña la jurisprudencia en el panorama jurídico costarricense, tanto como evidentemente lo tiene la legislación vigente.

A partir de 1993, la Corte Suprema de Justicia de Costa Rica acordó iniciar un plan que tiene como meta fundamental la de contribuir con la modernización del Poder Judicial, a fin de adecuar la institución y los procedimientos jurídicos y administrativos a las exigencias actuales del ciudadano y de la sociedad civil. El objetivo es hacer realidad la exigencia constitucional de una justicia pronta, cumplida y sin denegación, como requisito indispensable para el desarrollo y mantenimiento de la democracia.

En el segundo semestre de 1994, una empresa consultora contratada al efecto realizó un diagnóstico del ámbito de la administración de justicia y formuló el "Proyecto de Establecimiento del Sistema de Informática Jurídica", que forma parte del Programa de Modernización de la Administración de Justicia y cuya finalidad es implantar un sistema informático de jurisprudencia y legislación en sentido amplio, así como proveer acceso a la información relativa a la doctrina jurídica.

En Costa Rica se han llevado a cabo ya diversos esfuerzos con el fin de facilitar el acceso a esas fuentes de información jurídica. A mediados de la década de los 80, el Centro de Administración de Justicia de la Universidad Internacional de la Florida (FIU) realizó una evaluación del Sector Justicia de Costa Rica, bajo los auspicios del Instituto Latinoamericano de las Naciones Unidas para la Prevención del Delito y el Tratamiento del Delincuente (ILANUD) y el Proyecto Regional de Administración de Justicia (RAJO) de la A.I.D. Con base en dicho estudio, en 1988 se suscribió el acuerdo de asistencia entre la República de Costa Rica y los Estados Unidos de América para el Proyecto de Mejoramiento del Sector de Justicia (AID Proyecto Nº 515-0244 y sus anexos). El propósito de este proyecto bilateral fue el de consolidar y modernizar al Sistema de Justicia Costarricense fortaleciendo tres áreas de importancia, entre las cuales estaba la de contar con la disponibilidad de la información actualizada relativa a jurisprudencia, doctrina y legislación vigente.

Como organismo ejecutor del referido acuerdo de asistencia o proyecto bilateral se designó al ILANUD, mientras que el desarrollo de los sistemas correspondientes se encomendó a la Procuraduría General de la República (en cuanto a legislación), al Poder Judicial (jurisprudencia) y a la Facultad de Derecho de la Universidad de Costa Rica (doctrina).

Como resultado final de este convenio se cuenta actualmente con los recursos siguientes:

a) El ya mencionado SINALEVI de la Procuraduría General de la República, desarrollado con el software CA:GENERATOR, utilizando el administrador de bases de datos CA:DB/VAX, en equipos VAX de la empresa Digital.

b) En la Biblioteca de la Facultad de Derecho de la Universidad de Costa Rica se dispone de una base de datos de doctrina que utiliza el software MICRO-ISIS para almacenamiento y recuperación de la información.

c) En el Poder Judicial, la oficina del Digesto de Jurisprudencia, creada en el año 1973 con la finalidad de estudiar, clasificar y archivar las sentencias y compendios de jurisprudencia, así como elaborar diversos índices temáticos sobre este material. Desde ese entonces, se ha tratado de implantar un sistema automatizado que facilite tanto el almacenamiento como el acceso a los datos.

Concluido el proyecto de la AID, las diferentes instituciones continuaron –en la medida que les permitían los respectivos recursos presupuestarios, técnicos y humanos– con el desarrollo de aplicaciones e incorporación de contenidos en las diversas aplicaciones.

El SINALEVI está definido por la Ley Orgánica de la Procuraduría General de la República, en su artículo 41,

como "... el sistema informático–jurídico de la Procuraduría General de la República. En él se recopila, utilizando los medios tecnológicos adecuados, la legislación promulgada y vigente y se mantiene siempre actualizada. Además, se incorporan la jurisprudencia pertinente y cualquier otra información que precise y aclare el sentido de la legislación, con el objeto de que sirvan para desarrollar la labor consultiva y de abogado del Estado." Igualmente, se faculta a la institución para brindar este servicio a terceros interesados, ya sean públicos o privados.

Como resultado del Plan de Modernización del Poder Judicial, en mayo de 1994 se pensó en el replanteamiento del proceso de clasificación y sistematización de la jurisprudencia. Un año después se aprobó transformar el Digesto de Jurisprudencia en Centro Electrónico de Información Jurisprudencial (CEIJ), con el fin iniciar una nueva era de informatización de la jurisprudencia.

El CEIJ posee un sistema desarrollado en CLIPPER por el Departamento de Informática del Poder Judicial, que permite la introducción de los índices temáticos, descriptores, restrictores, el análisis jurídico respectivo y otros datos estructurados que identifican la sentencia. Dicho sistema, sin embargo, es limitado ya que no provee un módulo de actualización en línea que permita ingresar los índices temáticos y los extractos de las sentencias.

En febrero de 1995 se produjo la conclusión del Contrato de Préstamo 859/OC-CR para el Programa de Modernización de la Administración de Justicia, entre el Banco Interamericano de Desarrollo (BID) y el gobierno de Costa Rica, ratificado por ley número 7496, publicada en el Alcance nº 20 a La Gaceta nº 110 del 8 de junio de 1995.

De conformidad con lo establecido en ese convenio, el Poder Judicial –en su condición de "organismo ejecutor"– se abocó durante el segundo semestre del año 1995 a cumplir con las condiciones previas al primer desembolso. De esta forma, la Unidad Ejecutora del Programa Poder Judicial–BID inició sus operaciones de acuerdo con el plan de trabajo aprobado por el BID, en enero de 1996.

A la vista del desarrollo del referido Proyecto Corte–BID, se consideró que una de las necesidades prioritarias para el esfuerzo de modernizar el Poder Judicial, es el de poder suministrar información exacta, completa y en forma oportuna al juzgador; o sea, contar con un sistema de apoyo a la toma de decisiones. A pesar de la realización de todos los esfuerzos mencionados, aún no se ha llegado a consolidar la integración ni el acceso entre las fuentes señaladas, por lo que se requiere contar con un único sistema que a la hora de ser consultado por el usuario le integre la información de la jurisprudencia y la legislación.

DESCRIPCION DEL PROYECTO SCIJ

ALCANCE Y OBJETIVOS

El objetivo central del Sistema Costarricense de Información Jurídica es realizar una plena integración de la jurisprudencia y la legislación vigente, por vía de intranet (para los usuarios internos de las entidades participantes) e Internet (para el público en general). De esta manera, se permitirá a todos los interesados el acceso a toda la normativa (tanto vigente como histórica) sistematizada en el SINALEVI, así como a toda la jurisprudencia constitucional, de las Salas de casación y del Tribunal Superior de Casación Penal sistematizada por el CEIJ y el CISC, a través de una interface común.

Adicionalmente, el sistema mejorará la comunicación entre las instituciones involucradas, así como entre los despachos judiciales, las oficinas encargadas de la recopilación y clasificación de las sentencias.

En el ámbito de normativa, el SCIJ contendrá todas las leyes, decretos ejecutivos, reglamentos y demás legislación de carácter general. Para cada norma, se tendrá su historia completa, es decir, todas las reformas y afectaciones sufridas, además de sus diferentes versiones.

El SCIJ permitirá la realización de consultas transparentemente, desde la jurisprudencia a la normativa citada en cada sentencia, y viceversa, es decir, de la norma a todas las sentencias que citan dicha legislación. En particular, se podrá acce-

sar el texto completo de todas las sentencias de la Sala Constitucional que hayan afectado a una norma jurídica.

Si bien colocar normativa y jurisprudencia en Internet no es en sí novedoso, sí lo es hacerlo de manera integrada; es decir, estableciendo nexos entre normas, entre sentencias y entre éstas y aquéllas. Para lograrlo, será necesario desarrollar una intensa labor de clasificación y sistematización semiautomatizada, empleando elementos avanzados de informática jurídica tales como tesauros y generadores de sentencias.

ENTIDADES PARTICIPANTES

En su etapa primaria, participan entonces en el diseño y construcción del SCIJ:

- El Poder Judicial, representado por el Centro Electrónico de Información Jurisprudencial (CEIJ) y el Centro de Información de la Sala Constitucional (CISC).

- La Procuraduría General de la República, a través del SINALEVI.

  Una vez que el SCIJ esté en funcionamiento, el objetivo es posibilitar la integración de otras entidades que son también generadoras y a la vez consumidoras de información jurídica, como la Asamblea Legislativa, la Contraloría General de la República, el Tribunal Supremo de Elecciones, etc.

ETAPAS

El diseño y construcción del SCIJ comprende las siguientes fases:

1. Rediseño de procesos

La primera etapa es la del rediseño de los procesos y procedimientos de los diferentes entes involucrados en el proyecto, incluyendo el CEIJ, el CISC y el SINALEVI, así como el rediseño del flujo de información, entendido como la secuencia integrada de trabajo para recopilar, clasificar, almacenar y recuperar la información sobre jurisprudencia y legislación.

2. Definición de la solución informática

La segunda etapa es la definición de una solución informática. A partir de un modelo lógico del proceso, se busca encontrar la mejor solución informática para soportar el nuevo esquema. Se conceptualiza con base en la definición de una arquitectura del sistema informático, más una plataforma tecnológica sobre la cual trabajará la solución del sistema, tanto en el CEIJ como en el CISC y el SINALEVI. En esta etapa se establecen los requerimientos para ambos aspectos.

3. Desarrollo de la solución informática

La tercera etapa es la del desarrollo de la solución informática. Consiste en la construcción de sistemas informáticos que apoyarán los procesos de trabajo del CEIJ, la Sala Constitucional y la Procuraduría General de la República. Esta etapa incluye el análisis lógico, el diseño, la construcción de los programas, la prueba de sistemas, la capacitación a los usuarios del sistema y del personal de informática, así como el desarrollo de elementos para el plan de implantación.

4. Implantación

La cuarta etapa es la implantación de los nuevos procesos, esta vez soportados por el sistema informático (dual) que se construyó. Esta etapa se inicia con el diseño de un plan, en el que debe considerarse una etapa de aprobación del plan, la depuración y migración de los datos desde los anteriores sistemas informáticos existentes tanto en el SINALEVI como en el Poder Judicial, hacia los nuevos sistemas y la implantación definitiva.

5. Evaluación y ajustes

La quinta etapa es la de evaluación y ajustes a los procesos y procedimientos del sistema. El objetivo de esta etapa es corregir y adaptar el modelo para solucionar los problemas que se hayan presentado durante la implantación. Se especifican dos niveles de evaluación: el primero, de detección de problemas a nivel de procedimientos, de flujos y de sistemas, el segundo, a nivel de los resultados esperados. Ambos niveles permitirán obtener conclusiones respecto del proceso de rediseño general.

ESTADO ACTUAL

El proyecto se encuentra actualmente en la etapa de Desarrollo de la Solución Informática, en la subetapa de ejecución de pruebas de las aplicaciones. Se espera proceder a la instalación y prueba de las aplicaciones en junio del presente año. El SCIJ estará en línea y a disposición de los usuarios aproximadamente en agosto del presente año.

COMPONENTES

El SCIJ no consta de una aplicación monolítica, sino de catorce módulos desarrollados para atender a las diversas etapas del proceso de clasificación y sistematización tanto de normativa como de jurisprudencia, así como a las necesidades de las entidades participantes. Esos módulos son:

- SCIJ RNJ y Sala.dot[1]

Estas aplicaciones (la segunda es específica de la Sala Constitucional) facilitan el uso de un formato estándar preestablecido para las sentencias, incorporando automáticamente los datos necesarios para su posterior recuperación en el sistema.

- SCIJ-CONTROL-PGR y SCIJ-CONTROL-PJ

Facilitan el proceso de recopilación del material a incorporar en la base de datos tanto jurisprudencial como de normativa, automatizando el proceso de distribución entre los abogados encargados del proceso de análisis jurídico. También ofrece estadísticas sobre cuánta información se ha recopilado y cuánta está pendiente de clasificar y de incorporar en la base de datos.

- SCIJ SENTENCIAS

Coadyuva con el proceso de sistematización de las sentencias, incluyendo la definición de extractos y la clasificación por diversas materias jurídicas, según los términos existentes en el tesauro que también forma parte de la base de datos del sistema.

- SCIJ NORMATIVA

Esta aplicación permite la sistematización de la normativa, incluyendo la actualización de afectaciones de las leyes, clasificación y tipificación de las mismas haciendo uso del tesauro, así como creación de textos vigentes.

- SCIJ TESAURO

Permite la definición de un vocabulario jurídico controlado, para cada una de las distintas ramas del derecho, lo cual facilita la clasificación de las sentencias y normas por descriptores y restrictores, para poder realizar búsquedas más eficientes del tema requerido.

[1] Sobre la plantilla sala.dot se puede consultar la ponencia "Generación informatizada de sentencias en la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica", presentada separadamente a este mismo Congreso.

- SCIJ-PRONUNCIAMIENTOS

Esta aplicación permite la sistematización de los pronunciamientos de la Procuraduría General de la República, facilitando el enlace con la normativa que corresponda y con otra jurisprudencia relacionada.

- SCIJ-ASUNTOS CONSTITUCIONALES

Esta aplicación permite clasificar y relacionar la normativa con las acciones de inconstitucionalidad, consultas judiciales y consultas legislativas, que son presentadas, admitidas o resueltas en la Sala Constitucional.

- SCIJ-WEB NORMATIVA Y SCIJ-WEB JURISPRUDENCIA

Todas estas aplicaciones permiten la consulta vía Internet o intranet. Se establecen tres tipos de consulta: búsqueda selectiva por datos estructurados (como, por ejemplo, el número del expediente, número de sentencia, el magistrado o juez redactor), búsqueda libre por cualquier palabra dentro del texto de la ley o de la sentencia; y búsqueda temática por términos del tesauro.

- SCIJ-PUBLICACIONES PGR Y SCIJ-PUBLICACIONES PJ

Estas aplicaciones generarán reportes de la base de datos, facilitarán la elaboración de la Revista Constitucional, de la Revista Judicial y un Boletín conteniendo los dictámenes de la Procuraduría General de la República.

PROCESOS PRINCIPALES EN EL PODER JUDICIAL

RECOPILACION

Las Salas de la Corte y los Tribunales son los productores de los textos jurisprudenciales, los cuáles son enviados a través de la red judicial al Centro Electrónico de Información Jurisprudencial en el caso de las sentencias producidas por las Salas de Casación y los Tribunales y en el caso de la Sala Constitucional al Centro de Información de la Sala Constitucional (CISC). Para facilitar el proceso de recopilación de la información y su incorporación en la base de datos se desarrolló dos aplicaciones (RNJ y Sala.dot, mencionadas arriba) que permiten la redacción de las sentencias en un único formato estándar, enviando la sentencia a la base de datos del SCIJ con algunos datos estructurados que facilitan la posterior búsqueda de la información, tales como el número único del expediente, el número y fecha de la resolución, el nombre del magistrado, etc.

CLASIFICACION

El sistema facilita el proceso de clasificación de la información jurisprudencial a través de una aplicación que le permite a los abogados analistas de los entes sistematizadores de jurisprudencia (CISC y CEIJ) tipificar cada sentencia en las diferentes ramas del derecho, asignando descriptores que forman parte del vocabulario jurídico contenido en el tesauro del sistema. Adicionalmente, se hacen las ligas de las sentencias con la normativa citada y se crean máximas de las sentencias.

CONSULTA

La consulta se suministrará a través de los sitios web del Poder Judicial y de la Procuraduría General de la República, permitiendo al consultante navegar transparentemente de un sitio a otro cuando existan ligas entre las normas y la jurisprudencia. A través de un enlace electrónico entre los dos entes se facilita tanto el proceso de sistematización como de consulta, de manera que para el usuario final sea invisible el paso de una base de datos a otra. Se permiten búsquedas a través del texto completo de las leyes, búsquedas selectivas por los datos estructurados que identifican una sentencia o búsquedas temáticas a través del vocabulario jurídico controlado por el que se clasificó la información.

EN LA PROCURADURIA GENERAL DE LA REPÚBLICA

RECOPILACION

La información que alimenta la base de datos del SINALEVI, en lo que respecta a normativa, es suministrada por diferentes entidades. En el caso de leyes y decretos, existe un convenio entre la Procuraduría y la Imprenta Nacional para que la información de normativa publicada en el diario oficial "La Gaceta" sea enviada vía correo electrónico al SINALEVI y de ahí incluida en el SCIJ.

En cuanto a los asuntos constitucionales, tales como acciones de inconstitucionalidad, que de algún modo afectan o cuestionan la normativa vigente, esta información será suministrada al SINALEVI a través del enlace electrónico establecido para tales fines.

El otro tipo de información que recopila el SINALEVI son los dictámenes generados en la misma Procuraduría (que constituyen jurisprudencia administrativa) y ahí mismo incorporados en la base de datos.

CLASIFICACION

El sistema facilita el proceso de clasificación de las normas, dictámenes y asuntos constitucionales, presentando al abogado del SINALEVI la misma herramienta tesauro que utiliza el Poder Judicial. En el proceso de clasificación, los abogados se encargan de hacer las afectaciones a las leyes con base en sentencias de la Sala Constitucional o de nueva normativa. Además, los abogados analistas construyen los textos vigentes de las leyes y el sistema automáticamente maneja el concepto de "versiones", por medio del cual los textos históricos de las normas permanecen disponibles en la base de datos.

Con respecto a la información de los dictámenes, los abogados los tipifican por ramas del derecho y los clasifican en el mismo sentido que la jurisprudencia del Poder Judicial, agregando extractos, resúmenes y concordancias entre los mismos.

CONSULTA

La consulta de legislación ofrecerá la misma interfaz que tiene la aplicación web del Poder Judicial, permitiendo la búsqueda selectiva, por datos que identifican la norma (como número, nombre, ente emisor, etc.); la búsqueda temática a través de tesauro y la búsqueda libre a través del texto completo de las normas y dictámenes.

CONCLUSION

El SCIJ representa un gran esfuerzo tecnológico y de colaboración de las entidades participantes. Se espera que coloque al país a la vanguardia de la región en lo relativo a sistemas avanzados de información jurídica.

SOBRE LOS AUTORES

Carmen Quesada Chacón, costarricense, es licenciada en Ciencias de la Computación e Informática de la Universidad de Costa Rica. Encargada del proyecto Sistema Costarricense de Información Jurídica en la Unidad Ejecutora del Programa Poder Judicial- BID. Teléfono (506) 256-5668. Email: cortebid@sol.racsa.co.cr / Carmenquesada2@latinmail.com

Christian Hess Araya, costarricense, es licenciado en Derecho y máster en Ciencias de la Computación e Informática, ambos grados de la Universidad de Costa Rica. Letrado de la Sala Constitucional de la Corte Suprema de Justicia y profesor de Derecho Informático en la Universidad de La Salle, en San José. Miembro de la Association for Computing Machinery (ACM). Dirección postal: Apartado postal 239, Paseo de los Estudiantes. San José, 1002. Costa Rica. Teléfono: (506) 295-3902. Email: chess@poder-judicial.go.cr / chess@abogados.or.cr. Página web: www.geocities.com/SiliconValley/Circuit/1491/

La formación de la ley, las Bibliotecas Parlamentarias y las Nuevas Tecnologías

Autores: Rodrigo Obrador Castro (Chile)
Abogado
Magister c. en Ciencia Política
Biblioteca del Congreso Nacional - Chile

Patricia Reyes (Chile)
Abogado Coordinadora de Proyectos
Candidata a doctor "Comunicación, Derecho de la Informacion y Etica en América Latina y España".
Universidad Complutence de Madrid
Biblioteca del Congreso Nacional - Chile

INTRODUCCION

La Modernización del Estado en el contexto de un sistema democrático, con su correspondiente división de funciones; Ejecutiva, Legislativa y Judicial nos sitúa en el centro de la temática referida al modelo organizacional y funcional del Estado, con particular incidencia del avance registrado hasta hoy y proyectable a futuro, de las nuevas tecnologías de información y comunicación.

El desafío del Estado es implementar las tareas imprescindibles para la sociedad, y que por su naturaleza sólo él puede realizar, por ejemplo: liderar las relaciones internacionales, ya sea con otros países o con organismos internacionales; detentar, dirigir y organizar el monopolio de la fuerza socialmente organizada, esto es Fuerzas Armadas y de Orden; algunas atribuciones regulatorias; y diseñar e implementar, a través de los ministerios sociales, proyectos de rentabilidad social, en áreas como la educación, salud, vivienda, etc.

Pero este desafío del Estado, no sólo se limita a detectar estas necesidades e implementar soluciones, es necesaria la máxima eficiencia y eficacia del aparato estatal para optimizar los resultados, y en este sentido es indispensable la incorporación de herramientas y procesos de tecnología de punta que permita en definitiva satisfacer el fin último del Estado, cual es mejorar la calidad de vida de los miembros de la sociedad.

DEMOCRACIA REPRESENTATIVA; HETERONOMIA Y AUTONOMIA EN RELACION A LA NORMA JURIDICA

Una moderna línea de argumentación, explicativa del fundamento de la democracia representativa es la denominada "Teoría liberal del mandato representativo". Los elementos que es necesario considerar en esta explicación teórica son: En primer lugar, la categoría de "mandato" que surge a partir de un esquema ideológico propio del siglo XVIII, pues esta figura se adecua a la necesidad de legitimar el poder, haciendo aparecer como mero mandatario al representante pues quien gobierna es la nación. En segundo lugar, debe tratarse de un mandato "Nacional", esto es que el representante debe serlo no de su circunscripción electoral sino de la nación como totalidad. En tercer lugar debe tratarse de un mandato "General", esto coincidente con las ideas de Constant referidas a la división especializada del trabajo, así tiene sentido que la actividad potencial del representante libere de esta misma actividad potencial a los representados. En cuarto lugar es necesario señalar que debe tratarse de un mandato "Libre" esto es amplísimo. En quinto lugar, y como consecuencia de lo hasta aquí desarrollado, se trata de un mandato "no responsable", la única sanción eventualmente aceptable es la no reelección en el cargo.

Es propio de un sistema democrático, que los ciudadanos, según los mecanismos establecidos por el sistema electoral, designen representantes que conforman el Poder Legislativo. Esta democracia representativa permite a los ciudadanos, a través de sus representantes, establecer las normas que los rigen. Importancia central en esta materia tiene el considerar que el ejercicio democrático es, en este sentido, una fuerte atenuación al carácter de heteronomía de la norma jurídica.

Básicamente la norma jurídica es heterónoma en cuanto, la voluntad que genera la norma y por cierto, su contenido es distinta a la que en definitiva resulta obligada por la misma. Aquí radica la importancia de un sistema democrático y su ejercicio, pues en este sistema existe un acercamiento entre la voluntad generadora de la norma y

la definitivamente obligada por la misma, en cuanto son los propios ciudadanos, quienes a través de sus representantes, participan en el proceso de formación de la ley y de la determinación de su contenido; así el carácter de heteronomía de la norma jurídica se ve matizado con cierta autonomía, entre la voluntad emisora de la norma y la voluntad regulada por la misma. Esto encuentra su importancia en que este margen de autonomía importa un espacio de libertad y un margen decisional para los ciudadanos. Es por este espacio de libertad y voluntad de los ciudadanos que tiene central relevancia el funcionamiento del Poder Legislativo, y específicamente el proceso de formación de la ley, el cual debe ser eficiente, eficaz y tecnológicamente actualizado. Esto significa, en última instancia, un sistema democrático más libertario y participativo.

EL PROCESO DE FORMACION DE LA LEY

El proceso legislativo puede definirse como el conjunto de "etapas", que ordenadas de acuerdo a lo establecido en la Constitución Política del Estado y en el resto de la legislación intermedia pertinente, permite la aprobación o rechazo de los proyectos de ley sometidos a la consideración del Congreso Nacional.

Para estos efectos en Chile entendemos por "etapa" el conjunto determinado de eventos a través de los cuales se obtiene el pronunciamiento de cada una de las Cámaras, de las Comisiones Mixtas, del Tribunal Constitucional y del Presidente de la República, sobre el contenido de un proyecto.

Una gestión moderna, en cualquier ámbito, público o privado debe incorporar el uso adecuado de las nuevas tecnologías de información.

Por otra parte, la posibilidad de los Parlamentos de recibir y transmitir en forma oportuna la información necesaria para el desarrollo de sus actividades propias, así como la oportunidad de conocer de modo inmediato las experiencias de entidades semejantes en diversos ámbitos, a través de las potencialidades inherentes a las nuevas herramientas tecnológicas, conforma sin duda un escenario de enormes posibilidades de desarrollo organizacional y de gestión.

En este marco es que debe destacarse la reciente iniciativa del PARLATINO en virtud de la cual la presidencia del mismo fue designada como el órgano político del proyecto de informática que tiene por objeto fortalecer a los Parlamentos Nacionales de América Latina tanto en forma individual como en su interrelación, promoviendo su cooperación mediante el establecimiento de un sistema de información parlamentaria común

La nueva responsabilidad fue tema de la reunión de la junta directiva del PARLATINO realizada en Sao Paulo. Los programas involucrados en el proyecto informático incluyen: a) Legislación Latinoamericana b) Parlamentarios c) Instituciones d) Estadísticas e) Partidos Políticos f) Sociedad y g) Servicios y Productos. En este sentido se solicitó a todos los Congresos miembros la firma del proyecto de convenio que se está elaborando y que se proceda a la capacitación de los funcionarios pertinentes.

Otras experiencias interesantes son: la del Foro Parlamentario del Asia Pacifico que ha creado una base de datos legislativos que tiende a promover el intercambio legislativo, y la experiencia desarrollada por la Unión Interparlamentaria Mundial a través de un programa para el estudio y promoción de las instituciones representativas, en este cuadro compila y entrega información a los parlamentos, constituyendo una base de datos de características peculiares.

BIBLIOTECAS PARLAMENTARIAS

En la práctica resulta funcionalmente coherente que las modernas Bibliotecas Parlamentarias ejerzan una función importante en lo relacionado con el almacenamiento, procesamiento y recuperación de la información relevante al quehacer legislativo. Esta labor se lleva a cabo fundamentalmente a través de la mantención de bases de datos bibliográficos, legislativos (normas jurídicas vigentes y proyectos de ley), y últimamente con el desarrollo de lo que se ha denominado las "Bibliotecas Virtuales", esto es la posibilidad de acceder a través de Internet a un sitio

Web, que contiene información propia y conexión, vía alianzas estratégicas, a otras Instituciones que disponen de la información que requieren sus usuarios. Estas alternativas importan una nueva vía de acceso a la información y un potencial de usuarios creciente.

Un desafío actual para las Bibliotecas Parlamentarias es lograr una mayor presencia, con todo su aporte de conocimientos y tecnología, al proceso de formación de la ley.

Con este objeto estas organizaciones trabajan actualmente en establecer los mejores mecanismos de gestión de la información para el apoyo directo a dicho proceso.

Algunas herramientas tecnológicas desarrolladas en Chile por la Biblioteca del Congreso Nacional, de uso frecuente en la actividad Parlamentaria son: Sistemas de Bases de Datos Bibliográficos (EFESO), Sistemas de Bases de Datos Legislativos (SIJL), Sistema Integrado de Información Legislativa (SINILEG); Biblioteca Virtual (www.congreso.cl/biblioteca.html); Sistemas de información de Prensa en Línea etc. Por otra parte la cantidad y calidad de la información que se entrega se enriquece con Bases de Datos Extranjeras (Colecciones en CD actualizables, acceso vía convenios a través de Internet a páginas de contenido relevante para la actividad legislativa),

SINTESIS

En el contexto general de la temática de la Modernización del Estado, resulta de importancia, la referencia al proceso legislativo, por cuanto en una Democracia Representativa el contenido de las normas jurídicas, representan un espacio de libertad y voluntad para los ciudadanos. Así todas las iniciativas tendientes a revestir el proceso legislativo de mayor eficiencia, eficacia y transparencia conllevan un fuerte sentido democratizador, en el escenario descrito, cobran significado las actividades de las Bibliotecas Parlamentarias que incorporando tecnología a la gestión de información relevante para el proceso en referencia, hace en definitiva un aporte para la consecución del fin señalado.

Sistema de Información Jurídica Legislativa DE LA Biblioteca del Congreso Nacional

Presentaremos a continuación, el Sistema de Información Jurídica Legislativa (SIJL), desarrollado por la Biblioteca Congreso Nacional de Chile, como ejemplo práctico de un producto de información en formato electrónico, que pretende apoyar la labor de los legisladores en el proceso de formación de la ley, así como las actividades de todos y cada uno de los usuarios de la Institución.

El SIJL es un sistema integrado de información que permite el almacenamiento, procesamiento y recuperación de documentos jurídicos bajo la forma de legislación positiva chilena. El Soporte Tecnológico está constituido por:

- Una base de datos relacional
- Corre en ambiente Windows
- Sistema Administrador Basic Plus
- Tres diferentes aplicaciones: LEX BCN, Legis, Web Legis

Las Funciones del SIJL son almacenar, procesar y recuperar legislación positiva chilena publicada en el Diario Oficial. Para estos efectos conforman el SIJL dos tablas, a saber: Texto de Normas; Indice de Modificaciones.

ALMACENAMIENTO

EL SIJL CONTIENE:

- Textos completos de normas jurídicas publicadas en el diario oficial
- Registro referencial de las vinculaciones de esas normas

En la tabla Texto de normas encontramos el texto original de las normas tal como ha sido publicado en el Diario Oficial o en otras fuentes autorizadas; y los textos actualizados con las modificaciones que ha experimentado la norma, en su última versión y versiones anteriores.

En cuanto a los tipos de normas almacenadas, se encuentran: la Carta Fundamental, los Códigos de la República de Chile, Leyes, Decretos leyes, Decretos con fuerza de ley, y otras normas de jerarquía inferior a la ley como Decretos, Resoluciones, Autos Acordados, Ordenanzas, etc.

DATOS ESTADISTICOS A ENERO DEL 2000

Total de normas ingresadas en texto completo:

- Textos Originales 88.183 normas
- Textos actualizados 4.790 normas

Total de registros en el índice de vinculaciones

Total 104.568 registros

PROCESAMIENTO DE LA INFORMACION

El procesamiento de la información comprende 3 procesos definidos: Ingreso de documentos al sistema, Composición de textos actualizados y Vinculación de los documentos almacenados en el Sistema.

PROCESO DE INGRESO

Es el proceso por el cual se selecciona, revisa e ingresa la información al SIJL. Comprende también la supervisión. El producto generado por este proceso es el texto original completo de la norma, almacenado en el Sistema.

El proceso descrito comprende las siguientes etapas: Depuración del Diario Oficial, Revisión del texto de la norma, Formateo del texto, Marcaje de las partes de la norma, Ingreso de datos identificatorios, Carga de la norma en el sistema y Supervisión.

PROCESO DE ACTUALIZACION

Es el proceso por el cual se compone un nuevo texto de una norma a partir de la modificación introducida por otra norma. El producto generado por este proceso es el texto actualizado de los documentos modificados de cada norma.

Las etapas de este proceso de actualización son: Análisis de los textos (modificatorio y modificado); Composición del nuevo texto; Ingreso del texto con sus respectivos alcances, y Supervisión

PROCESO DE VINCULACIÓN

Es el proceso por el cual se analizan e ingresan al SIJL las diversas relaciones existentes entre las normas jurídicas ya almacenadas en el sistema. Este proceso genera el Listado referencial de vinculaciones o Indice de Vinculaciones.

Las etapas involucradas en este proceso de vinculación son: Estudio de los textos y análisis del tipo de vinculación, Selección e ingreso de la vinculación en el sistema y Supervisión

RECUPERACION DE LA INFORMACION

La recuperación de información opera de distinta forma dependiendo del tipo de aplicación a utilizar:

LEGIS

Usuarios: Red interna (parlamentario, comisiones, funcionarios del Congreso Nacional de Chile)
Menú de búsqueda, contiene ayuda en línea
Formato de salida predefinido
Sólo consulta

WEB LEGIS

www.congreso.cl/biblioteca.html
Usuario de la red en Chile y en el mundo
Menú de búsqueda prediseñado
Formato salida predefinido

LEX-BCN

Usuarios especializados (analistas y referencistas)
Formularios de búsquedas y salidas autodiseñados
Habilitado para el ingreso y procesamiento de la información

Reflexiones sobre el Real Decreto 994/1999 y la Seguridad en Bases de Datos

Emilio Del Peso*, Mario G. Piattini** y Eduardo Fernández-Medina*** (España)

RESUMEN.

En este artículo mostramos una visión general sobre el recién aparecido Reglamento de Seguridad (Real Decreto 994/1999) que es un compendio de medidas de carácter organizativas y técnicas que velan por el cumplimiento de la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) (Ley Orgánica 5/1992)[1], tratando posteriormente las bases de datos seguras, y más concretamente las políticas de control de acceso más importantes en la actualidad. Además se exponen unas consideraciones sobre la importancia de adaptar los sistemas de bases de datos al citado Reglamento de Seguridad, estableciéndose estrategias para realizar diseños de bases de datos que incluyan requisitos de seguridad acerca del nivel de clasificación que dicta el mencionado Reglamento de Seguridad, y que permitan, aprovechando las características de algún tipo concreto de bases de datos facilitar la labor de llevar a cabo las medidas de seguridad.

1. INTRODUCCION.

El papel que está tomando la información en las empresas y organizaciones cada vez es más importante. Hasta el punto de que a menudo el éxito o incluso la supervivencia de las empresas dependen de la calidad y la gestión de la información. Para garantizar la estabilidad de la información es necesario establecer ciertos mecanismos de seguridad, tanto de índole técnica como organizativa, puesto que la información, que habitualmente se encuentra almacenada en bases de datos puede verse alterada por muchas causas, tanto involuntarias, como terremotos o incendios, como voluntarias o mal intencionadas, como robo de información, actos terroristas, accesos a información confidencial, modificación de datos clave, etc.

Realizando un análisis desde otra perspectiva, están apareciendo bases de datos con informaciones que se pueden considerar sensibles, puesto que hacen referencia a ciertos aspectos íntimos o personales que han de ser especialmente protegidos, como creencias religiosas, tendencias sexuales, datos médicos, etc., y que si se usan sin ciertas precauciones pueden violar la intimidad de los individuos.

En este artículo nos centramos en las medidas técnicas para garantizar la seguridad lógica de las bases de datos, más concretamente en asegurar que el diseño de bases de datos contempla la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (a partir de ahora , LOPD) mediante el cumplimiento de las medidas de seguridad indicadas en el Reglamento de medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (Real Decreto 994/1999), quedando las medidas organizativas y la seguridad física fuera del alcance del mismo.

El aspecto que aquí se trata es de suma importancia, no sólo por la importancia que tiene para las organizaciones salvaguardar la integridad, confidencialidad y disponibilidad de los datos, sino porque como se comenta en Peso (1999b), a pesar de que durante estos últimos años no se han podido aplicar penas a delitos relacionados con la protección de datos de carácter personal al no estar éstos incluidos en el antiguo código penal, con la entrada en

* Informáticos Europeos Expertos (IEE). Torpedero Tucumán, 28, 1º A. 28016, Madrid. Tel: 34 91 350 13 73. Fax: 34 91 350 60 53. edelpeso@iee.es. http://www.iee.es

** Escuela Superior de Informática. Universidad de Castilla-La Mancha. Ronda de Calatrava 5, 13071, Ciudad Real. Tel. 34 926 29 53 00 (ext. 3715) Fax. 34 926 29 53 54 e-mail: mpiattin@inf-cr.uclm.es. http://www.inf-cr.uclm.es

*** Fac. de Ciencias Jurídicas y Sociales. Universidad de Castilla-La Mancha. Cobertizo de San Pedro Mártir, s/n. 45071 Toledo. Tel: 34 925 268800 (ext. 5123). Fax: 34 925 26 88 01. e-mail: efmedina@jur-to.uclm.es. http://uclm.es

1 La Ley Orgánica 5/1992, de 29 de octubre (LORTAD) ha sido derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal. El Reglamento de medidas de seguridad aprobado por el RD 994/1999 ha quedado subsistente según la Disposición transitoria tercera de la LOPD 15/1999 hasta tanto el Gobierno de acuerdo con la Disposición final primera apruebe o modifique dicho Reglamento para la aplicación y desarrollo de dicha Ley.

vigor de la Ley Orgánica 10/95 de 23 de noviembre, las infracciones que se venían cometiendo contra la LORTAD y ahora contra la LOPD y que, por su gravedad, tengan carácter penal, ya pueden ser sancionadas.

Los primeros estudios sobre seguridad en bases de datos se centraron en el control de acceso discrecional, que define las restricciones de acceso basadas en la identidad del usuario. Más tarde surgió el control de acceso requerido u obligatorio, que tiene controles de seguridad más exigentes que el discrecional y le da cierta autonomía a los datos, al adquirir éstos un nivel de seguridad propio. Para soportar el control de acceso obligatorio surgieron las bases de datos multinivel, que clasifican los datos de acuerdo con el nivel de seguridad que se les asigna.

2. REGLAMENTO DE SEGURIDAD.

Según el Real Decreto 994/1999, la LOPD, como antes hacía la LORTAD prevé en su artículo 9, la obligación del responsable del fichero de adoptar las medidas de índole técnica y organizativas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana del medio físico o natural, estableciéndose en el artículo 44.3.h) que mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen constituye infracción grave en los términos previstos en la propia Ley.

Sin embargo, hasta la aprobación del Reglamento de Seguridad no ha sido posible disponer de un marco de referencia para que los responsables promovieran las adecuadas medidas de seguridad y, en consecuencia, ha sido imposible hacer cumplir uno de los más importantes principios de la Ley Orgánica.

El Reglamento determina las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

El Reglamento consta de 6 capítulos, el primero con las Disposiciones Generales, el segundo con las medidas de seguridad de nivel básico, el tercero con las de nivel medio, el cuarto con las de alto nivel, el quinto relativo a las infracciones y sanciones, y el sexto, que establece las competencias del Director de la Agencia de protección de datos.

En los artículos 1 y 2 se establecen los objetivos ya comentados arriba, y una serie de definiciones de conceptos básicos como sistema de información, usuario, recurso, autenticación, etc.

En el artículo 3 se considera la clasificación de los datos según la naturaleza de los mismos en cuanto a necesidades de seguridad, estableciéndose tres niveles, básico, medio y alto.

En el artículo 4 se indican cuáles son los archivos que pertenecen a cada nivel, además de afirmar que para cada archivo, atendiendo al nivel a que pertenezcan, se han de aplicar las medidas de seguridad correspondientes a tal nivel y las de los niveles inferiores:

- Nivel básico: Todos los archivos que tengan datos de carácter personal.

- Nivel medio: Ficheros que tengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, hoy 29 de la Ley Orgánica 15/1999. Introduce una categoría de datos la de servicios financieros que no aparecen en la Ley ni definen en ningún sitio.

- Nivel alto: Los ficheros que tengan datos especialmente protegidos (de ideología, religión, creencias, origen racial, salud o vida sexual), así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas. Según la LOPD se incluye también la afiliación sindical.

Además, cuando los ficheros tengan datos de carácter personal que permitan obtener una evaluación de la personalidad del individuo tendrán que cumplir las medidas de seguridad expuestas en los artículos del 17 al 20 correspondientes al nivel medio. Esto es tan subjetivo que puede llegar a crear inseguridad jurídica.

Un resumen de los distintos niveles de seguridad a aplicar, dependiendo del tipo de datos de que se trate aparece en la Figura 1 (García, 1999).

En los artículos 5, 6 y 7 se dice que para trabajar con ficheros con datos de carácter personal a través de redes, o fuera del local donde estén ubicados, o si se trata de ficheros temporales, se tomarán las medidas de seguridad adecuadas a su nivel de seguridad. Además, si son ficheros temporales, éstos serán destruidos una vez hayan dejado de ser necesarios.

Nivel Básico: Incluye los tipos de datos de carácter personal pero que no permitan crear un perfil del individuo

Medidas de seguridad de Nivel Básico

Medidas de seguridad de Nivel Medio

Medidas de seguridad de Nivel Alto

Identificativos
Características Personales
Circunstancias Sociales
Académicos y Profesionales
Empleo y Carrera Administrativa
Información Comercial
Económico-financiera
Transacciones

Nivel Medio: Datos de carácter personal que permiten crear un perfil de las personas

Hacienda Pública
Servicios Financieros
Solvencia Patrimonial y Crédito
Infracciones Penales y Administrativas

Nivel Alto: Datos especialmente protegidos o recabados para fines policiales

Ideología
Creencias
Religión
Origen Racial
Salud

Figura 1. Niveles de Seguridad.

En el nivel básico, se exigen los siguientes aspectos, que también serán exigidos por los niveles medio y alto:

- Artículo 8. Documento de seguridad. Tiene unos contenidos mínimos, que son, el ámbito de aplicación con especificación de los recursos protegidos, las medidas, normas, procedimientos, reglas y estándares para garantizar la seguridad, las funciones y obligaciones del personal y los procedi-

mientos de notificación, gestión y respuesta ante las incidencias. El encargado de redactar este documento, así como de difundirlo es el responsable del fichero.

- Artículo 9. Funciones y obligaciones del personal: Serán definidas las funciones y obligaciones del personal así como las posibles sanciones que pueden recaer sobre ellos para evitar futuras confusiones e injusticias.

- Artículo 10. Registro de incidencias: Para que en el futuro se puedan averiguar las posibles anomalías que han ocurrido en cada momento, es necesario implantar un registro de incidencias en el que para cada una aparezca el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se lo comunica, y los efectos que se han derivado de la misma.

- Artículo 11. Identificación y Autenticación: Ha de existir una relación actualizada de usuarios que tengan acceso al sistema, debiendo establecerse procedimientos de identificación y autenticación para el acceso a éste. Cuando el mecanismo de autenticación sean contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Cada usuario cambiará periódicamente su contraseña

- Artículo 12. Control de acceso: Los usuarios del fichero tendrán acceso únicamente a aquellos datos y recursos informáticos que precisen para el desarrollo de sus funciones, y que el responsable del fichero se encargará de evitar que usuarios no autorizados accedan a la información. Además, sólo personal autorizado podrá conceder o modificar privilegios a otros usuarios.

- Artículo 13. Gestión de soportes: En los soportes donde se almacenan los datos, ha de aparecer información para identificar el tipo de datos que contiene, han de ser inventariables y además, han de estar almacenados en un lugar donde sólo los autorizados puedan acceder a ellos, siendo el responsable de los ficheros el único que pueda autorizar la salida de los soportes fuera del edificio de la organización.

- Artículo 14. Copias de respaldo y recuperación: Es labor del responsable del fichero verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de datos.

Además de las medidas anteriores, para los ficheros de nivel medio se consideran las siguientes medidas adicionales.

- Artículo 15. Documento de seguridad: Se amplía con respecto al requerido para nivel básico con algunos aspectos como la identificación del responsable de seguridad, etc.

- Artículo 16. Responsable de seguridad: Para controlar y coordinar las medidas definidas en el documento de seguridad, el responsable del fichero deberá designar uno o varios responsables de seguridad.

- Artículo 17. Auditoría: Los ficheros de nivel medio, y por lo tanto los de nivel alto han de ser sometidos una auditoría interna o externa que verifique el cumplimiento del Reglamento y demás aspectos de seguridad cada dos años.

- Artículo 18. Identificación y autenticación: El responsable del fichero tendrá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y verificará que está autorizado. Además, no se permitirá que un usuario intente reiteradamente accesos no autorizados al sistema.

- Artículo 19. Control de acceso físico: Sólo el personal autorizado en el documento de seguridad

podrá tener acceso a los locales donde se encuentren los sistemas de información con datos de carácter personal.

- Artículo 20. Gestión de soporte: Se aumenta la información que hay que gestionar sobre el soporte y sobre las personas receptoras del mismo en caso de envío. También exige que cuando se vayan a desechar o reutilizar soportes, se tomen las medidas oportunas para evitar que se pueda obtener información de tales soportes de manera ilícita.

- Artículo 21. Registro de incidencias: Se indica que cuando se realicen procedimientos de recuperación de datos, se ha de almacenar información sobre la persona que ejecutó el proceso, sobre los datos restaurados, y sobre los datos para los que haya sido necesaria una grabación manual.

- Artículo 22. Pruebas con datos reales: Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten de ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se lleven a cabo las medidas de seguridad acordes al nivel de seguridad correspondiente al tipo de fichero.

Las medidas a tomar para los ficheros de alto nivel son todas las medidas anteriores mas las siguientes:

- Artículo 23. Distribución de soportes: La distribución de los soportes que contengan datos de carácter personal se realizará cifrando la información contenida en los mismos o utilizando otro mecanismo que garantice que la información no sea inteligible ni manipulable durante el transporte.

- Artículo 24. Registro de accesos. Será obligatorio documentar todos los accesos que se produzcan. De cada acceso se guardarán como mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso, y si ha sido autorizado o no el acceso.

- Artículo 25. Copias de respaldo y recuperación: Se amplía el de nivel medio, exigiendo que se conserven las copias de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente (otro edificio) de aquel en que se encuentren los equipos informáticos que los tratan.

- Artículo 26. Telecomunicaciones: La transmisión de datos personales a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable por terceros.

En el artículo 27, referente a infracciones y sanciones, se especifican los artículos de la LORTAD modificados por la LOPD a los que hay que remitirse a la hora de detectar infracciones, y para decidir el procedimiento para imponer una sanción.

El artículo 28 obliga a los responsables de los ficheros a tomar las medidas organizativas y técnicas para preservar la seguridad en los ficheros con datos de carácter personal.

El último artículo, el 29, delimita las competencias del Director de la Agencia de Protección. Según Peso (1999b), la Agencia de Protección de Datos que nace como un organismo independiente que se encarga de garantizar el cumplimiento de las previsiones y mandatos establecidos en la LORTAD, garantizando así los derechos de los afectados respecto a sus datos de carácter personal (Peso, 1999a).

Según se afirma en la Disposición transitoria única, una vez aprobado este Reglamento, para las nuevas aplicaciones, las medidas de seguridad serán obligatorias pasado un plazo dependiendo del nivel de seguridad de los ficheros: 6 meses para nivel básico, este plazo se amplió tres meses por el RD 195/2000, de 11 de febrero, un año para nivel medio y dos para alto. Para el caso de aplicaciones en construcción que no permitan tomar las medidas de seguridad a corto plazo, el plazo máximo para adoptar tales medidas será de 3 años.

Como se afirma en García (1999), una vez que ha entrado en vigor del Reglamento de Seguridad, los informáticos han de cumplirlo de la siguiente forma:

- Comprobando que las aplicaciones faciliten la marcha de la legislación.
- Construyendo sistemas que desde el principio cumplan el Reglamento de Seguridad.
- Realizando recogida de información para encuestas, y destrucción de los cuestionarios personales según indique el Reglamento.
- Clasificando la información para decidir qué nivel de seguridad hay que aplicar.
- Aplicando el deber de secreto de los administradores de sistemas, redes, bases de datos y personal con acceso a datos de carácter personal.
- Conociendo todo lo referente a la legislación asociada a la protección y seguridad de los datos de carácter personal.
- Redistribución de personal entre áreas de seguridad informática y auditoría informática.

Con la entrada en vigor del reglamento, se dispone de un marco de referencia que permite que se tomen las medidas técnicas y organizativas para garantizar el cumplimiento de la LORTAD, hoy LOPD, y así garantizar también la seguridad de los datos de carácter personal. No obstante, no es suficiente disponer de tal marco de referencia, sino que hay que llevar a cabo las medidas que se proponen. Para garantizar que se cumplen las medidas propuestas en el reglamento, aparece en el artículo 17 la obligación de realizar auditorías de la seguridad para ficheros de nivel medio y alto. Precisamente las auditorías nos pueden ayudar a darnos cuenta de que algunas decisiones tomadas pueden ser erróneas, o se pueden incumplir contratos o incluso la propia legislación, que puede traducirse en grandes multas en el caso de infracciones graves, o lo que es aún peor, la inmovilización de los ficheros prevista en la LORTAD y actualmente en la LOPD (Piattini y Peso, 1998).

En Peso y Ramos (1998) y (1999) se puede encontrar un amplio estudio sobre la LORTAD y el Reglamento de Seguridad de la LORTAD y en Peso (2000) un análisis de la LOPD.

3. POLITICAS DE CONTROL DE ACCESO.

En este apartado se analizan las distintas políticas de control de acceso existentes, y su grado de adecuación a las medidas de seguridad que dicta el Reglamento.

Habitualmente se realiza el control de acceso de los usuarios a los recursos a través de reglas de autorización, que son tuplas con el siguiente formato <s,o,a>, que indican que el sujeto s puede actuar sobre el objeto o realizando la acción a.

Los sujetos son las entidades a los que se puede autorizar el acceso a los objetos, y aunque habitualmente son los usuarios individuales, también pueden ser grupos de usuarios, roles o incluso procesos que se ejecutan en nombre de los usuarios.

Los objetos son los elementos cuyo acceso queremos controlar. En el caso de sistemas de bases de datos relacionales, los objetos pueden tener distinta granularidad, es decir, se puede acceder a relaciones completas, a vistas o a atributos individuales.

Las acciones son las posibles operaciones que se permiten realizar, y que en bases de datos relacionales habitualmente son el select, el insert, el delete y el update.

3.1. Control de acceso discrecional.

Esta estrategia para gestionar el control de acceso es la más antigua, y está basada en la idea de que los sujetos acceden a los objetos en base a su identidad y a unas reglas de autorización, que indican para cada sujeto, las acciones que puede realizar sobre cada objeto del sistema. Con esta estrategia, si un usuario desea realizar una operación sobre un objeto, se busca en el sistema una regla de autorización que le de permiso para realizar esa operación sobre ese objeto, y si no se encuentra se le deniega el acceso.

Como se indica en Ferrari y Thuraisingham (2000), este mecanismo de acceso tiene las siguientes variantes que no son mutuamente excluyentes:

- Autorización Positiva y Negativa. Según la autorización positiva, la existencia de la regla de autorización indica que se puede realizar el acceso, mientras que la no existencia de la misma prohibe el acceso. En cambio mediante la autorización negativa, el acceso se permite sólo cuando no existe una regla de autorización negativa, mientras que la existencia de la regla prohibe el acceso. La principal diferencia es que en el caso de autorización positiva, si un sujeto no tiene autorización, en algún momento se puede producir una propagación de privilegios de tal forma que otro sujeto le ceda el acceso, en cuyo caso estaría burlando el control de acceso. Eso no puede suceder con el mecanismo de autorización negativa.

- Autorización Fuerte y Débil. Autorizaciones fuertes, tanto positivas como negativas son aquellas que no pueden ser invalidadas, mientras que las débiles si pueden ser invalidadas, de acuerdo a unas reglas específicas por otras autorizaciones fuertes o débiles.

- Autorizaciones Explícitas e Implícitas. Las autorizaciones implícitas son automáticamente derivadas por el sistema desde el conjunto de autorizaciones explícitas, de acuerdo a un conjunto de reglas. Las autorizaciones implícitas pueden ser derivadas mediante dos mecanismos: Mediante un conjunto de reglas de propagación, basado en una jerarquía soportada en el modelo o mediante un conjunto de reglas de derivación definidas por el usuario, permitiendo el otorgamiento de una autorización condicionada a la presencia o no de otra autorización. Por ejemplo, una regla de derivación puede ser usada para expresar que un sujeto puede acceder a un objeto dado sólo si otro sujeto tiene un acceso explícito denegado.
  Existen diferentes políticas de propagación de autorizaciones dependiendo entre otras cosas del tipo de sujeto de que se trate. Por ejemplo, si se trata de roles que forman una jerarquía, al asignar una autorización positiva, ésta se propagaría hacia todos los roles superiores en la jerarquía, y si la autorización es negativa, se propagaría hacia los roles inferiores en la jerarquía. En cambio, si se trata de grupos, la aproximación más utilizada consiste en la propagación de la autorización, tanto si es positiva como si es negativa a todos los elementos del grupo.

- Autorizaciones basadas en el contenido. Condicionan el acceso a un objeto dado al contenido de uno o más de sus componentes. Por ejemplo, restringir el acceso de datos de personas que cobre más de 50 millones al año.

Esta política de control de acceso también ha sido aplicada para bases de datos orientadas a objetos. Para este paradigma, han surgido diversas variantes de autorización como la 'heredada', donde a un usuario que tiene acceso a una clase, se le permite al mismo tiempo el acceso en las subclases correspondientes, a los atributos heredados de la clase, el 'Acceso a clase', donde el acceso a una clase completa implica el acceso a los atributos definidos en la clase, así como a los heredados por las superclases, y la 'visibilidad', donde un atributo definido en una subclase no es accesible desde ninguna de sus superclases (Piattini, 1994).

Esta política de control de acceso ha sido ampliamente utilizada, pero la autorización o no de cada uno de los intentos de acceso dependerá exclusivamente de la existencia o no de una regla de autorización, sin tener en cuenta el nivel de sensibilidad que tengan los datos. Además, existe un mecanismo de otorgamiento de autoriza-

ciones que permitiría dar acceso a ciertos datos a un usuario que antes no lo tenía, violando de esta manera la confidencialidad de los datos. Estas justificaciones hacen pensar que el control de acceso discrecional no es adecuado para que los sistemas de bases de datos cumplan con la clasificación que propone el Reglamento de Seguridad de la LORTAD hoy subsistente en la LOPD.

3.2. Control de acceso obligatorio.

Esta política de control de acceso está basada en el modelo diseñado por Bell y LaPadula para sistemas operativos, y consiste en la clasificación de tanto los sujetos como los datos en diversos niveles de seguridad como pueden ser 'sin clasificar', 'confidencial', 'secreto' y 'alto secreto'.

Las dos reglas básicas que definen la forma de acceder a los datos mediante esta política, adaptadas al paradigma de las bases de datos, indican que un sujeto tiene acceso de lectura a un objeto si el nivel de seguridad del sujeto domina sobre el del objeto, y que un sujeto tiene acceso de escritura a un objeto si el nivel de seguridad del sujeto es el del objeto, es decir, un sujeto puede modificar objetos de su nivel.

La principal característica de esta política de control de acceso es que un acceso es autorizado si existe una cierta relación entre el nivel de seguridad del sujeto y el del objeto al que se desea tener acceso. Además, los datos tienen niveles de seguridad por sí mismos, con independencia de quienes accedan a ellos (Piattini, 1993).

Para poder soportar esta política de control de acceso, es necesario utilizar unas bases de datos especiales que clasifiquen los datos por niveles. Estas bases de datos se conocen como multinivel, y soportan el control de acceso obligatorio a través de diferentes niveles de seguridad en los datos y diferentes niveles de acreditación para los usuarios. Cada nivel de seguridad tendrá componentes jerárquicos como los ya comentados anteriormente (alto secreto, secreto, confidencial, no clasificado). Cada nivel puede también tener categorías no jerárquicas como finanzas, ventas, investigación, etc.

No hay demasiado consenso en el tamaño de los datos que se clasifican en diversos niveles de seguridad en el caso de los sistemas de bases de datos relacionales. Los objetos que se pueden clasificar en niveles de seguridad, en un sistema de gestión de bases de datos relacionales atendiendo a su tamaño o granularidad podrían ser: Bases de datos enteras, relaciones o tablas, tuplas o filas de las tablas o bien elementos simples de datos o atributos.

Si podemos clasificar las tuplas en distintos niveles de seguridad, podría pasar lo siguiente: Supongamos que disponemos de una relación con los atributos CodigoEmpleado, Nombre, Apellidos, Cargo y Salario. Y supongamos también que una tupla se considera incluida en el nivel de seguridad conocido como 'alto secreto' cuando tiene un salario mayor de 120.000 $. Podríamos tener una tupla de 'alto secreto' con estos datos (123, José, Galán Rodríguez, Director, 200.000). Si alguien clasificado en el nivel de seguridad 'secreto' (que no tendría acceso a esta información) intenta insertar una nueva tupla con los datos (123, José, Galán Rodríguez, Director, 50.000), el sistema produciría un error indicando que ya existe una tupla con esa clave y esos datos. La información que el sistema le está dando a una persona clasificada en un nivel 'secreto' le estaría proporcionando conocimiento clasificado como 'alto secreto', puesto que estaría indicando que la persona que tiene esos datos tiene un sueldo mayor a 120.000$, puesto que desde su nivel de clasificación no puede ver esa información. Estaríamos perdiendo seguridad.

Para solucionar el problema anterior, ocasionado por la posibilidad de poder clasificar las entidades en distintos niveles de seguridad, es necesario utilizar una técnica llamada 'poli-instanciación', que consiste en poder tener varias versiones de la misma entidad. En principio, podría parecer incorrecto, ya que se repetiría la clave principal, y resultaría una violación de integridad. Esto se soluciona formando una nueva clave principal, con la clave antigua y el nivel de seguridad, de tal forma que cuando se repite varias veces una entidad, siempre estarán en niveles de seguridad distinto, y por lo tanto la clave principal será distinta. De esta forma, si se da el caso anterior, el problema se resolvería aceptando la inserción de la nueva tupla y así no tendríamos violación de integridad puesto que para la primera tupla la clave sería (123,AltoSecreto), y para la segunda sería (123,Secreto). Un análisis en profundidad sobre la poli-instanciación se puede encontrar en Jajodia, et al. (1995) y en Castano, et al. (1994).

A lo largo de estos últimos años han aparecido una serie de arquitecturas para soportar el control de acceso en bases de datos multinivel. Éstas se caracterizan entre otras cosas por la mayor o menor confianza en las medidas de seguridad que aporta el sistema operativo, para así delegar mayor o menor cantidad de aspectos de seguridad en el sistema de gestión de bases de datos. Las principales arquitecturas consideradas son las siguientes: a) Arquitectura de núcleo simple, donde es el sistema operativo el que se encarga de gestionar la seguridad. b) Arquitectura distribuida, según la cual se dispone de unas máquinas donde los datos están clasificados atendiendo al nivel de seguridad de los mismos. Hay dos modalidades, particionada y replicada. c) Arquitectura fiable o de confianza. Es el sistema de gestión de bases de datos el que se encarga de llevar a cabo todas las actividades de seguridad en lugar de hacerlo el sistema operativo. d) Arquitectura de cerrojo de integridad, que considera una máquina donde están los datos, otra que actúa de interfaz con el usuario, y un filtro que se encarga de la encriptación y la transmisión segura. e) Arquitectura de núcleo extendido, en la que tanto el sistema operativo como el sistema de gestión de bases de datos realizan un control de seguridad. (Ferrari y Thuraisingham, 2000).

Utilizando esta estrategia, vemos que podríamos tener los distintos niveles de clasificación que son propuestos por el Reglamento de medidas de Seguridad. En las líneas anteriores se habla de los niveles 'sin clasificar', 'confidencial', 'secreto' y 'alto secreto', y trasladando estos niveles a los recomendados por el Reglamento serían 'sin clasificar', 'nivel básico', 'nivel medio' y 'nivel alto'. De esta forma, mediante el control de acceso requerido y mediante las bases de datos multinivel podríamos organizar la información para que sean cumplidas las normas marcadas por la LOPD, y además el propio sistema de gestión de bases de datos podría gestionar de manera automática casi la totalidad de las medidas de seguridad en función del nivel de seguridad en los que se han clasificado los datos.

Es necesario disponer de un modelo que permita, tanto a los diseñadores como a los usuarios, plasmar explícitamente sus requisitos de seguridad, al igual que se hace con otros aspectos semánticos como la integridad del universo de discurso. En la Figura 2 exponemos un ejemplo utilizando un modelo entidad-interrelación extendido con algunos aspectos sobre la clasificación de los datos inspirados en el modelo SDMS ("Semantic Data Model for Security"), propuesto en Smith (1990) y (1991).

En el ejemplo aparecen tres entidades, Paciente, que se considera clasificada en el nivel básico por contener información de carácter personal, y Enfermedad y Consulta, que a nivel conceptual se consideran sin clasificar, por no tener datos de carácter personal. Aparecen dos interrelaciones clasificadas en el nivel alto, por considerar que están asociando datos de carácter personal con datos médicos (considerados estos últimos como especialmente protegidos por el Reglamento de Seguridad). Además aparecen unos cuantos atributos, algunos de los cuales están clasificados en el nivel básico por ser de carácter personal, otros no están clasificados (a pesar de ser datos médicos, en la entidad no se encuentran asociados a ningún enfermo), y otros pertenecen al nivel alto, puesto que pertenecen a una asociación entre datos de carácter personal y datos médicos.

Una vez que el esquema entidad-interrelación se transforme al relacional, cada atributo se clasificará de acuerdo a lo especificado en el esquema entidad-interrelación, y las tablas que surjan de la transformación también serán clasificadas de acuerdo al nivel del atributo con más requisitos de seguridad. Una solución para identificar el nivel de seguridad de los atributos o las tablas consiste en añadir al principio de los nombres siglas identificativas del nivel en el que se encuentran. Otra solución para clasificar los atributos sería añadir por cada uno, otro atributo que represente el nivel de seguridad, pero sería añadir demasiada redundancia, puesto que todos los elementos de una misma fila tendrán el mismo nivel de seguridad. En la Figura 3 se muestra el resultado de transformar a relacional parte del esquema entidad-interrelación anterior.

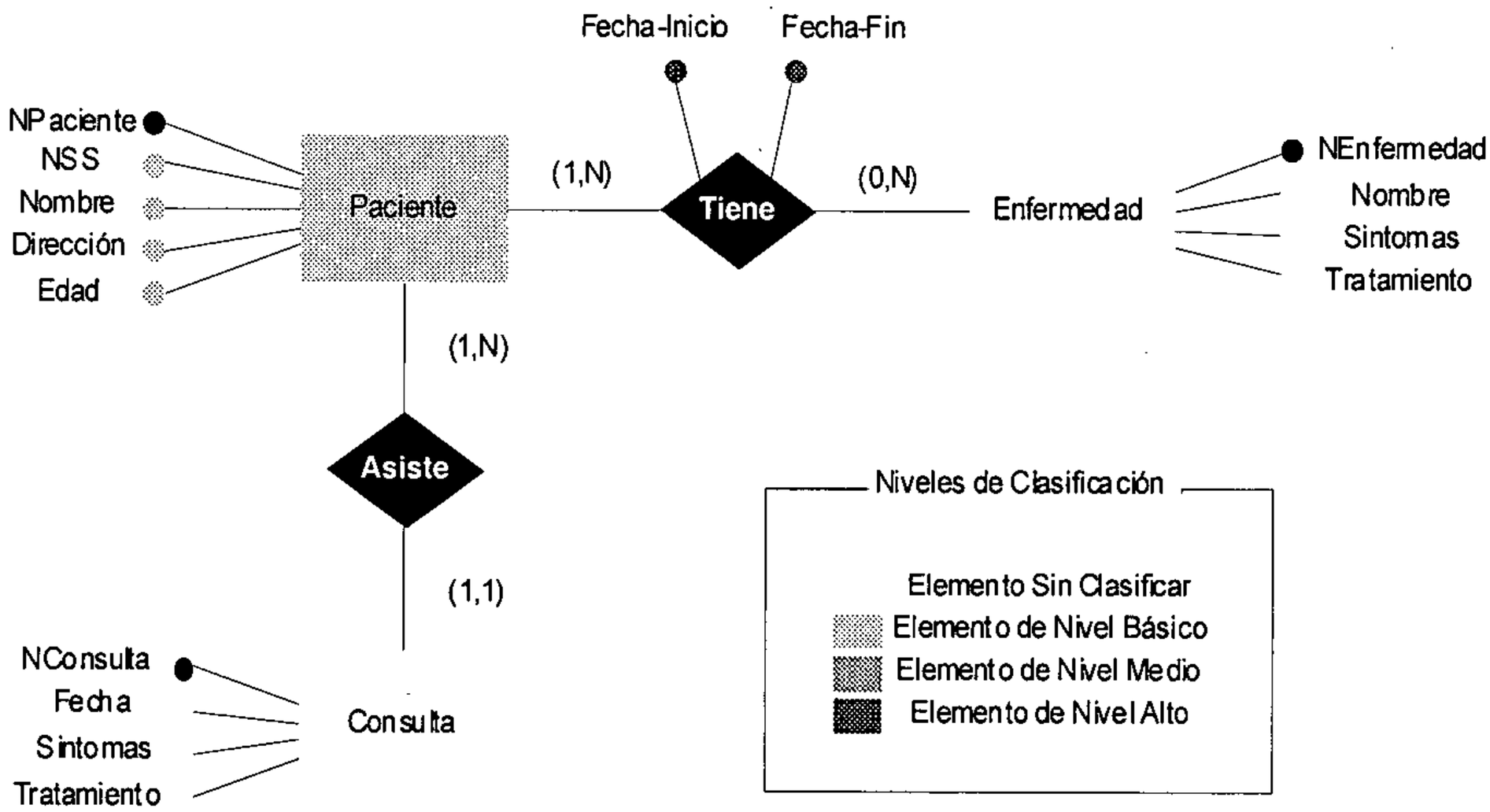


Figura 2. Ejemplo de Esquema Entidad-Interrelación con aspectos de Seguridad.

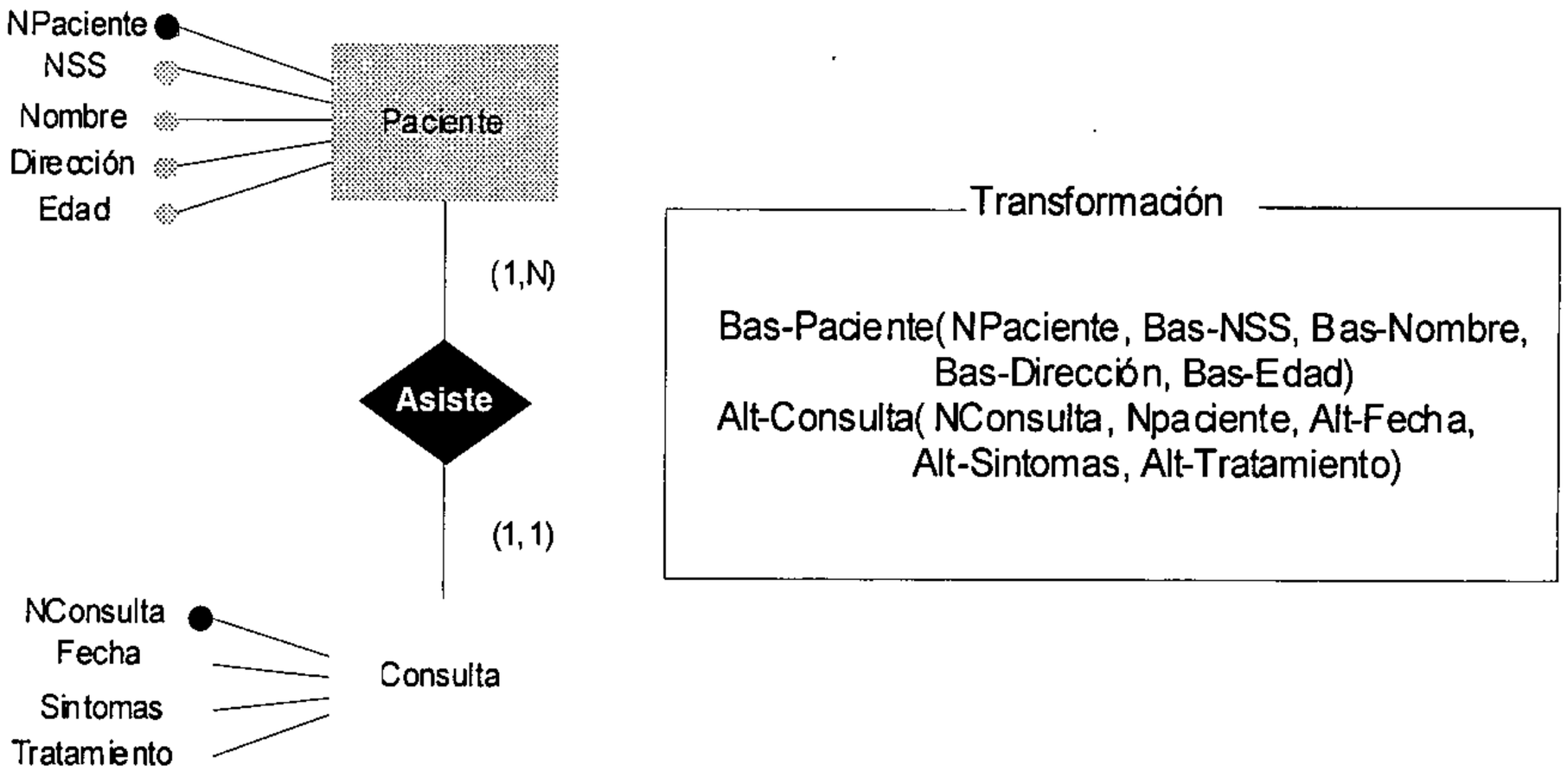
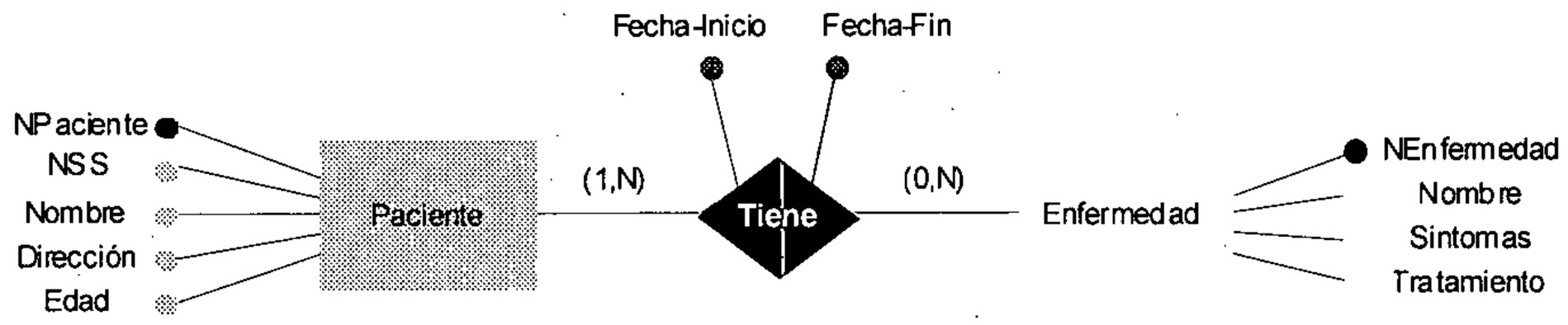


Figura 3. Transformación de entidad-relación a relacional (a).

La entidad Consulta, que en el esquema entidad-interrelación estaba sin clasificar, puesto que no contenían datos de carácter personal, al realizar la transformación pasa a ser una tabla clasificada en el nivel más alto, puesto que se ve afectada por la interrelación que asocia datos de carácter personal con datos médicos. En la figura 4 podemos ver la transformación del resto del esquema entidad-interrelación de ejemplo.

En esta transformación vemos que la interrelación muchos a muchos da lugar a una tabla clasificada en el máximo nivel, mientras que la entidad Enfermedad sería una tabla sin clasificar, puesto que no contiende datos de carácter personal.

Esta estrategia se podría llevar a cabo utilizando las bases de datos multinivel, y dándole funcionalidad a éstas para que gestione automáticamente las medidas de seguridad para cada tabla o fichero según su nivel de clasificación. Por ejemplo, aspectos como la identificación y autenticación, control de accesos, copias de respaldo, registros de incidencias, así como avisar al responsable de la necesidad de realizar auditorías son actividades que se podrían realizar de una manera automática, y en cierta profundidad de acuerdo con el nivel de clasificación de los datos, asegurándonos así de que se cumple la ley, y de que gozamos de una buena seguridad, que puede ser la garantía de supervivencia en muchos casos para las organizaciones.



Bas-Paciente(NPaciente, Bas-NSS, Bas-Nombre, Bas-Dirección, Bas-Edad)
Sin-Enfermedad(NEnfermedad, Sin-Nombre, Sin-Sintomas, Sin-Tratamiento)
Alt-Tiene(NPaciente, NEnfermedad, Alt-Fecha-Inicio, Alt-Fecha-Fin)

Figura 4. Transformación de entidad-relación a relacional (b).

4. CONCLUSIONES.

Los negocios actuales han creado una excesiva dependencia de las tecnologías de la información y las comunicaciones y se han hecho especialmente vulnerables debido, en gran parte, a las características propias del tratamiento telemático; vulnerables, en principio, por la falta de seguridad física que ello conlleva; vulnerables, también, por la falta de seguridad lógica y vulnerables, por último por la falta de seguridad jurídica (Davara, 1999).

Hasta hace poco tiempo existía una ley de protección de datos de carácter personal, la LORTAD, pero no existían medidas que pudiesen tomar las organizaciones para garantizar el cumplimiento de la Ley. Con la aprobación del Reglamento de Seguridad hoy sustituida por la LOPD se pretende disponer de las medidas de índole organizativa y técnica que permitan garantizar la confidencialidad y la integridad de la información, y así preservar los derechos de los afectados. Ahora, que ya existen las medidas de seguridad que permitan garantizar el cumplimiento de la ley y a su vez disponer de una seguridad sana en las organizaciones, nos encontramos con que hay que llevar a cabo tales medidas adaptando los sistemas que tienen ficheros con información de carácter personal. Una estrategia para adaptarse al cambio es utilizar las bases de datos multinivel para realizar un control de acceso obligatorio teniendo en cuenta la clasificación de los datos propuesta en el Reglamento de seguridad y una clasificación paralela de los sujetos que tengan acceso al sistema.

Para ello será necesario realizar modificaciones en las metodologías de desarrollo como por ejemplo la propuesta por Sell y Thuraisingham (1993), MOMT (Multilevel Object Modelling Technique) para bases de datos orientadas a objetos y seguras.

5. BIBLIOGRAFIA.

Castano, S., Fugini, M. Martella, G. y Samarati, P. (1994) Database Security. Addison-Wesley.

Davara, M.A. (1999). Perspectivas del Derecho de las Tecnologías de la Información y las Comunicaciones. NOVATICA, Nº 139. Pp. 4-6.

Ferrari, E y Thuraisingham, B. (2000). Advanced Databases: Technology y Design. Capítulo 11: Secure Database Systems. Eds.: Piattini, M. y Díaz, O. Artech House. Londres.

García, R.M. (1999). Construcción de la confianza en la protección de los datos de carácter personal. NOVATICA, Nº 141. Pp. 28-32.

Jajodia, S, Sandhu, R. y Blaustein, B. (1995). Infomation Security, An integrated collection of essays. Capítulo 21: Solutions to the Polyinstantiation Problem. Eds.: Abrams, M., Jajodia, S. y Podell, H. IEEE Computer Society. California.

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. BOE núm. 262, de 31 de octubre de 1992.

Peso, E. (1999a). La protección de los datos de carácter personal. NOVATICA, Nº 139. Pp. 12-14.

Peso, E. (1999b). Las Tecnologías de la Información y las Comunicaciones en el Código Penal. NOVATICA, Nº 139. Pp. 15-22.

Peso, E. (2000) La Ley de Protección de Datos. La nueva LORTAD. Díaz de Santos. Madrid, 2000.

Peso, E. y Ramos, M.A. (1998). LORTAD, Análisis de la Ley. Diaz de Santos. Madrid.

Peso, E. y Ramos, M.A. (1999). LORTAD, Reglamento de Seguridad. Diaz de Santos. Madrid.

Piattini, M. (1993). Hacia las bases de datos más seguras: SGBD multinivel. Seguridad Informática, Nº 8, diciembre 1993. Pp. 22-26.

Piattini, M. (1994). Seguridad en Sistemas de Bases de Datos orientados al Objeto. Seguridad Informática, Nº 12, diciembre 1994. Pp. 24-26.

Piattini, M. y Peso. E. (1998). Auditoría Informática, un enfoque práctico. Auditoría de la Seguridad. Ra-ma. Madrid.

Real Decreto 994/1999, de 11 de junio, del Ministerio de Justicia. BOE núm. 151, de 25 de junio de 1999.

Sell, P. y Thuraisingham, M.B. (1993). Applying OMT for Designing Multilevel Database Applications. Actas de Seventh IFIP Working Conference on Database Security. Huntville, Septiembre.

Smith, G.W. (1990). The Semantic Data Model for Security: Representing the Security Semantics of an Application. Actas de Sixth Int. Conf. Data Engineering, IEEE, pp. 322-329.

Smith, G.W. (1991). Modeling Security-Relevant Data Semantics. Actas de IEEE Trans. On Software Engineering, Vol. 17. Nº 11, november, pp. 1195-1203.

Tema 4

MODERNIZACION DEL ESTADO, DERECHO E INFORMATICA

Orientaciones para la introducción de tecnologías de la información en el Poder Judicial

Héctor Mario Chayer (Argentino)

San Mauro Castelverde 2356 Quilmes
Prov. de Buenos Aires, Argentina
Tel/fax (54-11) 4280-2790

RESUMEN DEL CV:

Abogado (Universidad de Buenos Aires - diploma de honor); Prof. de Filosofía y Ciencias de la Educación; Especialista en Gestión de Sistemas de Información e Internet aplicados (Cepade - Univ. Politécnica de Madrid).

Ejercicio liberal de la profesión de abogado y amplia trayectoria docente. Con fuerte orientación en el asesoramiento para la implementación de Tecnologías de la Información y las Comunicaciones en entidades educativas, empresas e instituciones públicas, en particular Poderes Judiciales. Colaborador de Fores (Foro de Estudios sobre la Administración de Justicia) y Cenit (Centro de Estudios en Information Technology)

RESUMEN DE LA PONENCIA:

El Plan Nacional de Reforma Judicial, lanzado en diciembre de 1998 por el gobierno argentino, desarrolla un plan integral para la reconversión general del sistema de justicia sobre la base de un modelo que responda a los principios de inmediación, eficiencia, calidad y acceso a la justicia. Su capítulo VII se refiere a la implementación de las Tecnologías de la Información. La novedad de su propuesta consiste en la posibilidad de tramitar en forma digital tanto la elaboración como la recepción de documentos, las comunicaciones internas y externas y la producción de información para todos los actores del sistema judicial, con Internet como interfase entre la Administración Pública y los ciudadanos. Para ello formula explícitamente un conjunto de orientaciones de política informática o tecnológica, cuya adopción evitaría avanzar por ensayo y error en esta área.

1. INTRODUCCION: EL PLAN NACIONAL DE REFORMA JUDICIAL

En diciembre de 1998, el gobierno argentino lanzó un ambicioso Plan Nacional de Reforma Judicial[1]. El Plan contiene gran cantidad de material estadístico y datos empíricos referidos a la situación de la justicia. Reconoce múltiples antecedentes (Justicia y Desarrollo Económico, del Colegio de Abogados de la Ciudad de Buenos Aires y FORES, estudios de fuentes constitucionales, estudios previos como los del Banco Mundial y el BID como así también trabajos de FIEL y el IERAL, etc...). Aunque el origen directo del trabajo es el "Programa Modelo de Reforma para las Administraciones de Justicia Provinciales" (BID 925' OC-AR/ 1.EG.10) realizado entre los meses de agosto y octubre de 1998 por un equipo interdisciplinario de consultores.

Desarrolla un plan integral para la reconversión general del sistema de justicia sobre la base de un modelo que responda a los principios de inmediación, eficiencia, calidad y acceso a la justicia. Asimismo plantea dos bases esenciales, la flexibilización de la estructura jurisdiccional y la transparencia, para la revisión de las principales áreas que conforman el Poder Judicial. Propone un conjunto de orientaciones y líneas de acción e indica en cada caso el modo de su implementación. Parte del supuesto de que los problemas por los cuales atraviesa la justicia argentina, tanto nacional como provincial, básicamente no son de recursos financieros ni de dotación de personal, sino de falta de planificación y que el cambio debe producirse en base al mejoramiento del gerenciamiento de los recursos humanos, la flexibilización de las estructuras y la reconversión mediante la aplicación de las tecnologías de la información (TI).

[1] *Ministerio de Justicia de la Nación, Plan Nacional de Reforma Judicial. Buenos Aires Nov. 1999.*

Los ocho capítulos que conforman el cuerpo del trabajo desarrollan el plan de propuestas para cada una de las áreas en que se dividió la problemática:

Capítulo I. Objetivos. Se exponen los fundamentos que motivan la necesidad de la reforma y la búsqueda de inmediación, eficiencia, calidad y acceso a la justicia como principios rectores de las propuestas.

Capítulo II. Lineamientos de Política Judicial. Aquí se enuncian las pautas o líneas directrices para la reconversión del sistema. Se recomienda la creación de un Centro de Política Judicial y Control de Gestión en cada jurisdicción provincial y en el ámbito nacional, que podría depender de la CSJN o del Consejo de la Magistratura y sería el encargado del diseño de la política judicial.

Capítulo III. Lineamientos de Reforma para el Área Jurisdiccional. El área funcional importa la estructuración de los órganos jurisdiccionales; en este punto se analiza brevemente la situación actual de la utilización y funciones reales que cumplen los recursos humanos en la justicia.

Las propuestas giran en torno a tres ideas:

a) La reforma de la oficina judicial como unidad de "producción";

b) El desarrollo de un modelo de gestión judicial con la creación de oficinas comunes;

c) La división del trabajo por funciones, diferenciando los casos simples de los complejos.

También avanza sobre la modificación del horario judicial (en Argentina en general es de 6hs, sólo por la mañana), presentando distintas alternativas; y aborda la supresión de las ferias judiciales en los casos que implican la paralización de las tareas de los tribunales.

Capítulo IV. Lineamientos de Política de Recursos Humanos. Se focaliza sobre el entrenamiento del personal, teniendo en cuenta la implementación de las nuevas tecnologías y la creación de Escuelas Judiciales. Se destacan los avances en esta área del Poder Judicial de la Provincia de Córdoba.

Entre las principales propuestas figuran:

- Crear sistemas objetivos y uniformes para el ingreso al Poder Judicial en base a un entrenamiento común, que establezca un orden de mérito entre los candidatos y otorgue facilidades para las personas de otras jurisdicciones.
- Organizar un sistema de gerenciamiento de recursos humanos
- Modificar el régimen laboral con el objetivo de garantizar una curva de ingresos adecuada.
- Crear un Código de Conducta Judicial

Capítulo V. Lineamientos de Política Presupuestaria, de Estadísticas, de Auditoría, y Control de Gestión. Entre otras iniciativas, introduce la figura del administrador judicial y propone trabajar sobre la base de presupuestos por programa o base 0. En materia de estadísticas propone la utilización de indicadores por centro de costos, por fuero y por juzgado comparables vertical y horizontalmente, con indicadores físicos y monetarios atinentes a la tipología delictual y sociológica y de diagnóstico y análisis de la organización y gestión judicial. Estos indicadores y forma de organización permitirán realizar una evaluación de performance del sistema que permita fijar metas, revisar su logro o no y reelaborarlas periódicamente.

Capítulo VI. Reconversión Edilicia. Propone reconvertir las estructuras existentes y construir nuevas con las atribuciones de flexibilidad, plantas libres y bajo costo y mantenimiento. Las tareas se llevarían a cabo mediante la convocatoria pública por antecedentes para croquis preliminares o anteproyectos sobre bases dadas a doble vuelta.

Capítulo VII. Implementación de las Tecnologías de la Información. En este capítulo, que más abajo se desarrollará en detalle, la meta propuesta consiste en la posibilidad de tramitar en forma digital tanto la elaboración como la recepción de documentos, las comunicaciones internas y externas y la producción de información para todos los actores del sistema judicial. Es decir, pasar del sistema actual, basado en el papel y el procesamiento manual de datos, a un sistema cuyo soporte principal sea el digital, a través de Redes Informáticas Judiciales conectadas a Internet, que permitan la consulta remota, vía web, de expedientes digitalizados. Formula un conjunto de recomendaciones en cuanto a la adquisición de hardware y software, a los sistemas de seguridad informática que deberán acompañar su instalación y funcionamiento a la capacitación de los recursos humanos para su utilización, que se pretende sirvan como guía en el accionar de los responsables del área tecnológica.

Capítulo VIII. Lineamientos de Reforma al Sistema Jurídico. Este capítulo analiza, entre otros puntos:

- los métodos alternativos para la resolución de conflictos;
- el acceso a la justicia, la mediación comunitaria y asistencia jurídica gratuita;
- las facultades jurisdiccionales a los abogados y notarios;
- la policía judicial;
- el sistema de tratamiento y abordaje de menores para su reubicación social;
- la mediación penal
- la creación de un Centro de Asistencia a la Víctima

También hace referencia a las reformas al sistema legislativo que deberán efectuarse para la implementación de la reforma, distinguiendo el nivel de leyes orgánicas y procesales, y los estatutos de los funcionarios y empleados de la justicia.

2. LAS TECNOLOGIAS DE LA INFORMACION Y EL DERECHO: LA IMPORTANCIA DE INTERNET

Una herramienta clave en el impacto decisivo de las Tecnologías de la Información en el Derecho ha sido Internet, la "red de redes". La habilitación de la oferta comercial de acceso público a Internet en julio de 1995 marcó un hito decisivo en la marcha de la "revolución digital" en la Argentina. El trascendente Decreto Nº 554/97 del Poder Ejecutivo Nacional, declara "de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial Internet, en condiciones sociales y geográficas equitativas, con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciones de la multimedia.". Iniciativas más recientes, como el Decreto del Poder Ejecutivo Nacional de diciembre de 1999 (hoy suspendido) que delegaba en el Correo Argentino (empresa privatizada) la asignación de un correo electrónico a cada ciudadano se inscriben, si bien en este caso con graves errores, en esta línea. Asimismo, también ha sido incluida la firma digital en el ordenamiento legal argentino (Resolución N° 45/97 de la Secretaria de la Función Pública y decreto del Poder Ejecutivo Nacional No 427/98; existe también un anteproyecto de ley en el Congreso de la Nación) como solución técnica para la garantía de integridad y no repudio de los documentos digitales. Esta evolución lleva a plantear en el Plan Nacional de Reforma Judicial la posibilidad de considerar a Internet como interfase entre la administración pública (el Poder Judicial en este caso) y los ciudadanos.

3. LINEAMIENTOS PARA UNA POLITICA INFORMATICA

Como descripción general del sistema, el Plan Nacional de Reforma Judicial concibe un núcleo de gestión digital de la oficina judicial, integrada en redes conectadas a Internet, con posibilidad de tramitar integralmente la

no sólo la elaboración de los despachos y autos en el tribunal, sino también la recepción de documentos (por ej., de las partes, o respuestas a oficios) en formato digital, las comunicaciones internas y externas y la producción de información oportuna para todos los actores del sistema judicial (registros centralizados de causas, estadísticas, presencia en Internet, consulta remota de expedientes, etc...). Son elementos estratégicos de este sistema la capacitación de los recursos humanos y un adecuado programa de implantación.

Queda claro que, como telón de fondo, se concibe un nuevo paradigma de administración de justicia a partir de la "revolución digital". Esto sin perjuicio de proponer, a la vez, el proceso gradual para alcanzarlo.

El arrollador avance de las TI deja obsoleto el objetivo de la informática de gestión judicial como la mera ayuda al despacho a través del procesamiento de textos y la consulta de jurisprudencia (sería pasar de la mecanografía mecánica a la mecanografía informática). Reconocer las características invasoras, abarcativas, cuestionadoras y transformadoras de estas tecnologías las constituyen en un factor estratégico que impican una transformación cualitativa en la administración de justicia.

Pero ello debe hacerse según un plan orgánico, superando la etapa de difusión anárquica de equipos y sistemas en el Poder Judicial, asumiendo una planificación centralizada de las ingentes inversiones que se requieren para obtener el máximo provecho. Resulta explicativo el ya clásico modelo de Nolan (formulado en varios artículos en 1973 y 1974[2]) que describe el proceso de crecimiento del sistema de información de una organización. Nolan habla de cuatro etapas básicas, a saber:

- Etapa de iniciación: se inicia el uso de computadoras por un pequeño número de usuarios para satisfacer necesidades básicas. El control está descentralizado o no existe; al igual que la planificación, que en el mejor de los casos es mínima.

- Etapa de expansión o contagio: se difunde el uso de computadoras, entre usuarios que experimentan con sus posibilidades, proliferando por tanto las aplicaciones. Se produce una rápida elevación de los costos.

- Etapa de formalización o control: con miras a racionalizar el crecimiento se introducen controles organizacionales, con criterios de coste – efectividad. Se centraliza el control y se advierten beneficios potenciales.

- Etapa de madurez o integración: Se ajustan los controles y la planificación, logrando una integración de las aplicaciones y la coordinación entre el Sistema de Información y los objetivos de la organización

Se relacionan entre sí al ser etapas sucesivas de crecimiento, pasando de una a la otra a través del aprendizaje organizacional: la experimentación de la etapa de iniciación permite pasar a la difusión por contagio, que permite a su vez que se difunda la tecnología antes de que se apliquen los controles, etc... En razón de que la experiencia o aprendizaje organizacional que se adquiere en cada una es indispensable para la siguiente, no puede evitarse el paso por cada una de las etapas; lo que no significa que no pueda planearse, administrarse y gestionarse eficazmente.

Los Poderes Judiciales argentinos han recorrido un buen trecho en el aprendizaje organizacional en estos términos, aunque lamentablemente en general sin planificación ni administración ninguna. La potencialidad de las Tecnologías de la Información para el trabajo judicial favoreció su veloz difusión entre los operadores del sistema, lo que nos permite considerar que a fines del siglo XX la etapa que Nolan llama de contagio está concretada. El Plan Nacional, según mi parecer, servirá para inaugurar la etapa de formalización en el uso de Tecnologías de la Información en los Poderes Judiciales.

---

[2] Citado por DAVIS, GORDON y OLSON, MARGRETHE, Sistemas de Información Gerencial. Editorial Mc Graw Hill. México 1995.

Para brindar organicidad entonces a la introducción de Tecnologías de Información, el Plan Nacional presenta un conjunto de orientaciones. Constituyen recomendaciones para formular explícitamente una política informática que evite avanzar por ensayo y error, en base al voluntarismo de una o dos personas, en proyectos cuya dimensión justifica claramente el esfuerzo de planificación.

Se transcribe a continuación una apretada síntesis, que enumera las recomendaciones de modo sistemático y permitirá comprender su aspiración de integralidad.

1. Adquisiciones- recomendaciones generales

1.1. Se recomienda atender a estándares tecnológicos actualizados, buscando componentes con amplia aceptación en el mercado, y por ende, con múltiples opciones a la hora de contratar servicios basados en ellos.

2. Hardware

2.1. Se aconseja el tendido de una Red Informática Judicial, compuesta por redes LAN en cada edificio judicial, enlazados a través de una red WAN en cada ciudad/departamento judicial, preferentemente con conexión única a Internet.

2.1.1. Cuando exista una infraestructura de telecomunicaciones de la administración estatal correspondiente, se recomienda integrar la red informática judicial a ella.

3. Software

3.1. INFRAESTRUCTURA OPERATIVA

3.1.1. Sistemas Operativos, redes y protocolos

3.1.1.1. Se utilizará un protocolo de comunicación ampliamente difundido que permita la interconexión de equipos preexistentes, la interconexión mediante redes públicas (Internet) o privadas, y que brinde seguridad y confiabilidad en las comunicaciones.

3.1.2. Sistema de gestión digital de expedientes

Las mediciones del impacto del uso de esta herramienta en la oficina judicial no son abundantes; las pocas que existen en orden a la agilización de las tareas son realmente llamativas. Se recomienda entonces adoptar un sistema de gestión digital de expedientes que en un entorno amigable permita el cumplimiento de las siguientes prestaciones (se detallan sólo las más relevantes):

3.1.2.1. Codificación, sorteo y asignación de procesos, con un código único de identificación para toda la provincia.

3.1.2.2. Gestión de documentos judiciales, aprovechando las capacidades de la base de datos para modelos, consultas de jurisprudencia, etc...

3.1.2.3. Las prestaciones hipertextuales resultan muy importantes para el ordenamiento lógico en expedientes complejos y/o muy voluminosos.

3.1.2.4. La base de datos, de tipo distribuido, deberá poseer capacidades de full text search basadas en campos específicos; soporte de referencias hipertextuales, y búsquedas sobre

el texto completo de cada expediente (concebido como conjunto de documentos digitales auténticos).

3.1.2.5. Recepción de documentos digitalizados, brindando soporte para todo tipo de archivos (texto, hipertexto, audio, imagen, vídeo).

3.1.2.6. Integración con herramientas de comunicación del tipo correo electrónico y navegación en Web para todos los usuarios del sistema, que permita el envío y recepción de documentos digitales con garantía de no repudio, integridad y confidencialidad, de modo normalizado.

3.1.2.7. Soporte de funcionalidades de consulta pública y masiva de expedientes y jurisprudencia a través de la red informática judicial e Internet.

3.1.2.8. Integración con un sistema informático de manejo documental de jurisprudencia y vinculado al SAIJ.

3.1.2.9. Emisión de los informes necesarios para la administración de justicia.

3.1.2.10. Deberá incluir un sistema de información estadística automatizado.

3.1.2.11. Generación de documentos digitales de formato no propietario, que permitan posteriores migraciones de aplicativo y la consulta con software disponible en el mercado.

3.2. Software de productividad

3.2.1. Se recomienda definir un standard de software de productividad que permita el intercambio de información producida en otros ámbitos con el sistema de gestión digital de expedientes, homogéneo dentro de cada jurisdicción, y compatible en el ámbito nacional.

3.3. Software administrativo

3.3.1. Se aconseja que el software administrativo de apoyo a la jurisdicción se seleccione entre reconocidos proveedores locales, o internacionales con representación en el país, evitando los desarrollos a medida.

3.3.2. Se recomienda incluir un sistema de información estadística automatizado también para esta área.

4. Presencia en Internet

4.1. A fin de proveer información sobre el Poder Judicial, ayuda al ciudadano y permitir la consulta de la base de datos de expedientes y de jurisprudencia, se aconseja desarrollar un sitio web único por Poder Judicial, que abarque todos los fueros, instancias y servicios.

5. Seguridad informática

5.1. El control de accesos deberá permitir la estricta categorización de usuarios con privilegios grupales (por ej. funcionarios de un tribunal o sala) e individuales (por ej., juez para las causas que administra).

5.2. Se deberá prever un procedimiento adicional, como la encriptación, para garantizar el acceso a documentación reservada exclusivamente a su autor.

5.3. Deberá realizarse un backup diario de la base de datos.

5.4. Dada la apertura de una réplica de la base de datos a la consulta por Internet, deberá garantizarse el máximo nivel de seguridad disponible contra violaciones de seguridad intencionales externas y prever políticas de detección de ataques exitosos.

5.5. Definir e implementar una política antivirus centralizada.

5.6. A los efectos de garantizar el no repudio, la autentificación del emisor y la integridad de los documentos digitales, tanto los emitidos por las partes como por el órgano jurisdiccional o terceros, se aconseja implementar un sistema de firma digital para los documentos cuya importancia lo requiera.

5.7. Elaborar planes de contingencia, que definan los riesgos que enfrenta el sistema informático en su conjunto y prevean la recuperación de la operatividad del sistema en plazos predefinidos.

6. Políticas de uso aceptable de los Recursos Informáticos

6.1. Deberá preverse una política de uso aceptable de los recursos informáticos, tendiente al uso de los mismos únicamente para lo que se tiene autorización; para los fines que han sido desarrollados y protegiendo su integridad y disponibilidad.

7. Soporte de Tecnologías de la Información

7.1. Se deberá prever asistencia técnica especializada permanente, para el mantenimiento preventivo y correctivo del hardware y del software.

7.2. Deberán crearse puestos de alto nivel de responsabilidad informático, tales como Administrador de red / Administrador de base de datos, cuya jerarquía (en función de las responsabilidades que asumen para el funcionamiento del órgano jurisdiccional) deberá analizarse en detalle.

8. Problemática del año 2000

8.1. Tanto el hardware como el software deberán cumplir con el requisito Y2K compliance, referido a la problemática del año 2.000.

A esta altura de los tiempos esta previsión ha quedado, felizmente, superada.

9. Capacitación de los Recursos Humanos

9.1. La capacitación judicial en TI abarcará desde el impacto de la revolución digital en el Derecho, hasta la operación de las aplicaciones informáticas específicas.

9.2. Para garantizar el respaldo indispensable para el éxito de semejante transformación, deberá comenzarse por los niveles superiores, con particular hincapié en las garantías de seguridad, eficiencia y confiabilidad de los sistemas a implementar; y debe alcanzar con carácter obligatorio y continuo a todos los integrantes del Poder Judicial.

10. Implantación de las Reformas – Método

10.1. Se aconseja conformar una "Comisión para la introducción de las Tecnologías de la Información en el Poder Judicial" que lidere el proceso, representando al Poder Judicial, abogados y ciudadanos, y con participación de expertos. Entre sus principales tareas deberían estar:

10.1.1. Realización de un diagnóstico completo del área de las TI

10.1.2. Redacción de las políticas informáticas a aplicar

10.1.3. *Promoción de acciones destinadas a impulsar el cambio cultural necesario.*

10.2. Deberá evaluarse la conveniencia o no del arancelamiento de determinados procesos que hoy lo están, para estimular los nuevos mecanismos de consulta de información en general, jurisprudencia y gestión de expedientes a través de Internet.

10.3. Se aconseja implantar las reformas con el método de aproximaciones sucesivas

10.3.1.Por períodos breves con objetivos precisos, será útil la implementación de proyectos piloto en los distintos fueros.

10.3.2.Se aconseja que en el método de aproximaciones sucesivas se utilice una doble gradualidad:

- por fuero / instancia / departamento judicial
- en los procesos a informatizar.

Se desarrollaría entonces una implementación en al menos tres fases, siendo los ejes de cada una de ellas los siguientes:

1. Instalación de redes LAN, capacitación del personal, e implementación del Sistema de Gestión de Expedientes (para el trámite interno).

2. Interconexión de las redes locales en redes WAN, y habilitación de la consulta remota de expedientes por Internet.

3. Migración definitiva del soporte papel al digital, con la presentación de escritos digitalizados por las partes y terceros.

4. ALGUNAS EXPERIENCIAS PROVINCIALES ARGENTINAS

Con el apoyo financiero del Banco Mundial y del propio presupuesto nacional, impulsado desde la ex Secretaría de Asistencia Financiera a las Provincias – hoy Secretaría de Provincias, del Ministerio del Interior del Poder Ejecutivo Nacional - se ha desarrollado una actividad tendiente a la reforma y mejoramiento de los estados provinciales en el marco de un proceso dinámico.

A fin de optimizar la administración de los estados provinciales, el mejoramiento de los sistemas de justicia es uno de los elementos básicos. Las metas que orientan este esfuerzo de Reforma pueden ser sintetizadas en el logro de Sistemas de Justicia Provinciales que se caractericen por su eficiencia, accesibilidad y calidad, de modo de contribuir en forma decisiva a la seguridad jurídica y en definitiva a la generación de inversiones que permitan un *desarrollo provincial sostenido.*

Esta voluntad compartida de modernización requiere de una acción conjunta y complementaria entre el Gobierno nacional y los Poderes Judiciales provinciales. Con tal motivo se ha desarrollado un conjunto de subproyectos de Modernización Judicial de los Poderes Judiciales Provinciales; se concedieron préstamos a los Poderes Judiciales de las provincias de Córdoba, Santa Fe, Salta y Corrientes a los fines de informatizar la gestión judicial, para la adquisición de hardware y compra o desarrollo (en el caso de Córdoba) de software.

Realizaremos entonces una análisis parcial, que deja de lado otras iniciativas no menos interesantes, tales como las de las Provincias de Buenos Aires, Río Negro, Neuquén, y las del Poder Judicial de la Nación en el fuero Civil, Comercial, etc... Abordaremos solo tres proyectos de informatización[3], hoy en curso en el marco arriba descripto (Salta, Córdoba y Santa Fe) que exhiben diverso grado de avance.

El Proyecto de Informatización de la Gestión Jurídica y Administrativa del Poder Judicial de Salta es el más adelantado, con un presupuesto estimado en $5.690.000.-. Es un ambicioso proyecto de informatización basado en un plan de desarrollo integral y de implantación gradual de sistemas y tecnologías. Abarca como componentes principales hardware, software, comunicaciones, y recursos humanos. Tiene por objetivo dotar de herramientas tecnológicas al Poder Judicial, básicamente a través del enlace la totalidad de las dependencias en redes locales interconectadas en una Red Judicial Provincial, para lograr la optimización de los resultados, agilizando los trámites judiciales, y coadyuvando a la jerarquización del servicio y a la seguridad jurídica en general (considerada como condicionante de los niveles de inversión). En particular, se propone como solución alternativa a la creación de nuevos juzgados. La licitación de hardware fue adjudicada en marzo de 1999 a Compaq Latin American; se compraron 162 estaciones de Trabajo y 25 servidores. Cada juzgado será equipado con una red LAN con un servidor, conectado a servidores por fuero, con 6 estaciones de trabajo en general, 16 en el caso de los juzgados penales de instrucción, 15 en los juzgados de menores y 10 en los correccionales. Es decir que al menos en esta etapa no se llegará a una PC por empleado. A la hora de escribirse estas líneas se encuentra pendiente de adjudicación el concurso para adaptación e implementación del sistema de software de gestión judicial.

El proyecto de Optimización de la Gestión Administrativa y Jurisdiccional del Poder Judicial de la Provincia de Córdoba – Informática De Gestión tiene por objetivo la incorporación de tecnología informática para dotar al Poder Judicial de Córdoba de un sistema de información integral que posibilite mayor eficiencia en la gestión judicial. El proyecto abarca tanto el área administrativa como la jurisdiccional; y dentro de ella se propone, en primer término, llegar a todos los Fueros y Distritos Judiciales a lo largo de tres etapas de un año cada una y con un costo estimado de $6.874.000.-. Para la adquisición de equipos electrónicos y sistema de cableado estructurado y comunicaciones de la primera etapa ya se ha convocado a licitación pública internacional. En segundo lugar se propone el desarrollo de un Sistema de Administración de Causas para la gestión automatizada del proceso, la reunión de información adecuada tanto para la consulta del estado de los expedientes como el control de gestión, y la implementación de un sistema de comunicación. Finalmente, contiene un componente menor de capacitación.

El Proyecto Integral de Modernización del Poder Judicial de Santa Fe pone miras de calidad en el intento de informatizar la gestión del poder judicial incluyendo la gestión de la oficina judicial, los grandes registros provinciales y una base de datos documental, así como también la producción automatizada de estadísticas. Los costos totales se estiman en $12.643.000.-. Se han realizado las previsiones técnicas para permitir la consulta remota de expedientes por Internet, circulación "forzada" del documento, emisión de notificaciones, producción de libros de registro, videoconferencia y recepción de escritos en formato digital; si bien no está previsto, es perfectamente posible establecer un sistema de codificación única. Los pliegos convocando a licitación pública internacional para la provisión de hardware y software se encuentran en elaboración. A los fines organizativos, el proyecto fue dividido en dos etapas: una primera etapa que apunta a la adquisición de los sistemas de aplicación y del equipamiento y software necesario para su control e instalación a prueba del Sistema de Gestión Jurídica, Sistema Documental y la conversión de sistemas existentes e integración de los mismos al Sistema de Gestión Jurídica, en caso de resultar posible. Se seleccionarán 14 dependencias piloto (una por fuero e instancia), a las que se proveerá de hard de al menos tres marcas distintas, donde implementar el soft de gestión. Servirá para determinar los requerimientos defi-

[3] Para este análisis ha sido de gran utilidad la publicación de GARAVANO, CHAYER, SCOTTO, RODRIGUES ESTEVEZ, CAMBELLOTTI y RICCI, Las propuestas de reforma al Sistema de Justicia en Argentina. Cd Rom, Buenos Aires 1999.

nitivos del equipamiento necesario para la utilización de los sistemas permitiendo el inicio de la segunda etapa (procediéndose al trámite licitatorio con antelación al fin de la primera). En esta segunda fase, se prevé la adquisición e instalación del equipamiento y las redes para la puesta en funcionamiento de los sistemas en la totalidad de las dependencias judiciales comprendidas en el proyecto.

Vale una observación interesante: en 1999 se impulsaron desde el Programa de Desarrollo Provincial que estamos describiendo dos nuevos proyectos: el Planeamiento Estratégico y la Revisión Integral del Modelo de Gestión de las Oficinas Judiciales, como etapas ineludibles antes de continuar avanzando con los ambiciosos procesos de informatización arriba descriptos. Se consideran insumos básicos para el desarrollo y ejecución de los préstamos ya concedidos a los Poderes Judiciales de las provincias de Córdoba, Santa Fe, Salta.

Esto muestra que (tardíamente) se ha tomado conciencia de un peligro que acechaba a estos planes: "informatizar la burocracia", de modo que tareas que antes se realizaban con máquinas de escribir, escritorios y largas colas en tiempos excesivos para la ciudadanía... ahora pasen a realizarse con PC, escritorios y largas colas... con las mismas demoras. Recordemos además que los rituales procesales en la Argentina responden a una tradición centenaria pocas veces revisadas, lo que hace temer, además, que se estén automatizando actividades que deberían suprimirse. No hay peor cosa que hacer bien lo que no debería hacerse.

Destacamos en particular la necesidad de revisar los modelos de gestión de las oficinas judiciales. Se trata del análisis de los flujos de trabajo en las oficinas en estado de mayor criticidad para que se incorporen las modificaciones necesarias para optimizar su funcionamiento y se constituya en guía para una adecuada incorporación de las tecnologías de la información a los procesos judiciales, de modo de asegurar que los sistemas informáticos a implementar lo serán bajo una organización integral y sistémica. Ni más ni menos que la búsqueda de mejoras incrementales en los procesos de trabajo o directamente "reingeniería de procesos" cuando aparezca como necesario. Así la organización de los despachos u oficinas judiciales ha venido a constituirse en un componente básico en los procesos de reforma judicial iniciados en el marco de este Programa.

"Do Estado: uma análise de sua evolução e o papel inevitável da informática em seu processo de adequação aos tempos atuais"

Carmen de Carvalho e Souza (Brasil)
Asesora Jurídica y Magistrada de Justicia Federal del Estado de Minas Gerais, Brasil

Na Grécia antiga utilizava-se o termo *"polis"* o mesmo que cidade, uma vez que suas aglomerações jurídica e politicamente organizadas não ultrapassavam os limites da cidade. Em latim, o termo "Estado", oriundo da palavra *"Status"* possuía a significação de situação, condição, diferentemente do que a empregamos atualmente. Os romanos se aproximaram do atual conceito de Estado, utilizando a terminologia *"status reipublicae"* ou ordem permanente da coisa pública. Porém, Maquiavel em seu *"Il Principe"* é que deu ao Estado uma acepção de unidade política total: "Todos os Estados, todos os domínios que tiveram e têm império sobre os homens são Estados e são ou repúblicas ou principados."

Hodiernamente, podemos compreender o Estado como sendo um agrupamento social politicamente organizado, gerido por objetivos em comum, obviamente segundo determinadas normas jurídicas em um território certo e definido, sob a total tutela de um poder soberano, representado por um governo independente. Assim sendo, a consolidação do Estado surge à medida em que coexistem interesses similares de uma coletividade e o devido ânimo de colocá-los em prática.

Consoante os dizeres de Jean Dabin em seu *"Doctrine Générale de l'État,* "chegou um momento em que os homens sentiram o desejo, vago e indeterminado, de um bem que ultrapassa o seu bem particular e imediato e que ao mesmo tempo fosse capaz de garanti-lo e promovê-lo. Esse bem é o bem comum ou bem público e consiste num regime de ordem, de coordenação de esforços e intercooperação organizada. Por isso o homem se deu conta de que o meio de realizar tal regime era a reunião de todos em um grupo específico, tendo por finalidade o bem público. Assim, a causa primária da sociedade política reside na natureza humana, racional e perfectível. No entanto, a tendência deve tornar-se um ato; é a natureza que impele o homem a instituir a sociedade política, mas foi a vontade do homem que instituiu as diversas sociedades políticas de outrora e de hoje. O instinto natural não era suficiente, foi preciso a arte humana". Esta é a essência primordial do Estado.

Destarte, conclui-se que os objetivos do Estado são a ordem e a defesa social, em suma, o bem estar social, o bem público; sendo os seus três elementos precípuos o povo, o território e o poder político. Nos dizeres de Darcy Azambuja, "Estado é a organização político-jurídica de uma sociedade para realizar o bem público, com governo próprio e território determinado." Dalmo de Abreu Dallari entende o Estado como sendo "organização jurídica soberana que tem por fim o bem comum de um povo situado em determinado território". Importante ressaltar que na correta acepção do termo Estado, mister se faz ressaltar que "o fenômeno estatal revela-se no elemento pessoal (Estado–Comunidade) como no elemento poder (Estado-aparelho ou Estado-poder)" nos dizeres de Kildare Carvalho.

Georg Jellinek em seu "Teoría General del Estado" apresenta uma análise interessante e objetiva da evolução histórica do Estado com fulcro no elemento histórico e nos seus elementos caracterizadores: o povo, o território e o poder político. Deste modo, para Jellinek a classificação dos tipos de estado é: Estado Oriental, Estado Grego, Estado Romano, Período Medieval e Estado Moderno.

A idade antiga ou estado oriental tinha como traços precípuos a teocracia, a monarquia absolutista, acarretando a nível social a exorbitante estratificação social e presença mínima dos direitos e garantias individuais. São exemplos de comunidades que vivenciaram este tipo de estado os egípcios, mesopotâmios, hebreus e judeus.

O estado grego tinha como pilares a igualdade de todos perante a lei; ausência de títulos e funções hereditárias possibilitando o livre acesso a todos os cidadãos às funções públicas e o direito à livre expressão, à palavra, à argumentação pública do cidadão comum das atividades do governo. Aqui o Estado era a *"Polis"* ou cidade, de território de menores extensões, constituída de cidadãos livres, estrangeiros e escravos, sendo que aos dois últimos não era reconhecida a cidadania. Deste modo, podemos concluir que, apesar dos pilares da democracia advirem do estado grego, a democracia grega difere da democracia atual, uma vez que não era reconhecido o sufrágio universal, em detrimento dos estrangeiros e escravos; portanto o princípio de igualdade não era de fato inteiramente reverenciado.

O estado romano caracterizava-se pela vasta extensão territorial, culto aos antepassados e valorização da família. Urge ressaltar aqui a separação entre o poder público e o privado, sobressaindo-se o poder político do qual fazem parte o *imperium*(autoridade), a *potestas*(poder organizacional) e *majestas*(enaltecimento do poder). Era latente nos romanos a reverência ao governo.

O período medieval se destacava pela inexistência de coesão do poder estatal, havendo uma concepção patrimonial e fragmentária do poder, onde o cristianismo se revelou com forte impacto.

O Estado Moderno surge como uma nova leitura do conceito estado, onde a presença do poder político era centrado nas mãos de um único indivíduo, a crítica à autoridade papal é contundente na reforma, há a ascensão da classe burguesa e o florescer do capitalismo. Pode-se afirmar que este Estado Moderno passou por várias mutações, consoante o momento histórico emqual o mundo se encontrava. Deste modo, podem se enquadrar dentre este gênero Estado Moderno as espécimes: Estado Estamental, Estado Absoluto(presença da monarquia absoluta e regras apenas se limitam pelo Direito Natural) e Estado de Direito(nasce a idéia de soberania popular, nascimento das constituições escritas, reconhecimento dos direitos fundamentais e da separação dos poderes, estado absenteísta).

Nos idos do pós guerra (1914-18) assiste-se a um período de transformações, quando vigora a crise da Democracia e a impopularidade do Estado de Direito, cuja característica precípua era ser um estado estático, com normas obsoletas, não adequadas às transformações econômicas e sociais, o homem percebe a dura realidade em que vive e a necessidade de uma urgente adequação deste Estado de Direito às novas transformações, ou seja das normas às cada vez mais latentes, alterações econômicas e necessidades sociais.

Nasce o Estado Social de Direito, o qual vem atender às constantes transformações decorrentes das novas condições sociais da civilização industrial e pós industrial visando também a sobrevivência do Estado nos tempos modernos. A instituição Estado é submetida a constantes pressões, a crises políticas permanentes, gerando crises sociais gigantescas, sendo que a história nos mostra que tais situações geralmente foram abafadas mediante a imposição de formas estatais totalitárias acarretando a supressão da liberdade, a violência constante, o império do terror, a política externa agressiva. Desta forma, se o Estado como instituição desejasse subsistir-se deveria primeiramente empenhar-se em controlar de modo permanente, os aspectos econômicos, sociais e culturais da sociedade. O estado social de direito apresenta como traço distintivo a empresarialidade (o estado participa com um capital privado em empresas mistas, promovendo a estatização das empresas), a primazia da função social da propriedade (a propriedade do bem é limitada pela função social do mesmo). Em suma, o Estado Social de Direito tem função eminentemente social, é o Estado das Prestações, tendo como função precípua zelar pelo bem estar social, para tanto destina parte do produto nacional bruto para tal. Os direitos individuais são limitados em prol da sociedade.

Nas últimas décadas do século XX vivenciamos um processo de mutações ainda maior onde o capitalismo impera, o socialismo se extingue e um novo fenômeno, a globalização, dita novas fórmulas de mercado com a crescente internacionalização da economia, o alargamento de fronteiras, a tecnologia é cada vez mais aprimorada, etc.. Deste modo, o Estado Contemporâneo passa por mutações, sendo um período de crise de identidade do mesmo, onde a necessidade de adaptação aos reflexos da globalização faz com que os pilares do Estado Social de Direito se percam em parte. Há um conflito do Estado-Nação, do estado que se confunde com suas fronteiras, do estado social (das prestações onde impera a primazia do social), do estado pseudo-intervencionista, do estado empreendedor, com atividades econômicas; com as mudanças cada vez mais rápidas, o Estado vem se tornando mínimo, havendo um enxugamento forçado da máquina estatal, onde não há mais lugar para o estado paternalista, das prestações sociais; o intervencionismo dá lugar às iniciativas privadas, sendo assim, a privatização das empresas impera; os mercados comuns atraem cada vez mais países, formando blocos gigantescos de livre circulação de mercadorias, moeda e alguns de pessoas; a legislação tem de se adaptar cada vez mais às leis internacionais, fomentando o Direito Internacional, etc.. Neste ínterim, surge o computador, principal ingrediente desta avalanche de transformações ocorridas a nível mundial na segunda metade do século XX.

Em um mundo atual não há mais lugar para uma máquina estatal poderosa, paternalista, de fortes subsídios sociais, o Estado caminha para o seu enxugamento, se tornando um Estado Mínimo, ou seja, devendo apenas manter a ordem e administrar a justiça, tarefas por si só, demasiado vastas. Mister se faz a adaptação da máquina

estatal aos tempos atuais não se olvidando de que o Estado é um meio, não um fim em si mesmo, sendo a sua essência precípua regular condutas, visando a realização individual e social do homem. De modo simplista, Herbert. Spencer em seu *"Essais de Politique"* exemplificou tal necessidade "será necessário, pois, que o Estado se descongestione, que se desipertrofiem seus órgãos, que a experiência, já tão longa e o bom senso convençam os indivíduos de uma divisão mais equitativa e racional do trabalho entre eles e o poder público".

A este Estado Mínimo, junte-se um poderoso aliado, a informática. A informática revolucionou o modo de vida humano, sendo impossível elencar exatamente todas as transformações operadas. Alavancada pela acessibilidade dos computadores pessoais a um número cada vez maior de pessoas, acarretando a democratização do acesso à informática, a nível individual, o cidadão obtém uma vasta gama de informações a uma rapidez nunca dantes dimensionada detendo, portanto, uma maior integração ao mundo. Consequência deste fato é a maior especialização do indivíduo e inevitavelmente, o desenvolvimento social e econômico. Com o advento da internet, entramos em um mundo dotado de uma agilidade equivalente à de um e-mail, onde informações são trocadas, processadas, decisões são tomadas, enfim, a interatividade exige uma agilidade com que nos habituamos ainda que involuntariamente, sendo esta, uma realidade inadiável da qual a máquina estatal não pode se eximir.

Em tal quadro, não há mais que se falar em um Estado cuja morosidade, burocracia, ineficiência e indecisão saltam aos olhos. Urge que seja levado a efeito um processo de modernização do Estado aos tempos atuais, minimizando sua máquina com o auxílio da Informática tanto no plano Executivo, bem como no Legislativo e judiciário. No Legislativo, é imperativo que seja elaborada legislação concernente à regulação da informática e problemas inerentes ao seu uso (vários países do mundo já passaram por esta etapa e estão em constante aprimoramento), bem como regulamentação concernente à adaptação do funcionamento da máquina estatal concomitantemente à informática. O Judiciário tem na informática, um importante aliado na tramitação dos processos, agilizando o julgamento dos mesmos e consequentemente, agilizando a aplicação legal.

Destarte, após esta breve exposição, não há outra conclusão a não ser a inevitabilidade do processo de modernização da máquina estatal, onde torna-se imperativa a sua minimização, sendo a informática presença inevitável, visando a sobrevivência do Estado.

REFERENCIAS BIBLIOGRAFICAS:

DALLARI, Dalmo de Abreu *in "Elementos de teoria geral do Estado"*. São Paulo, Saraiva, 1989

AZAMBUJA, Darcy *in "Teoria Ceral do Estado"*. São Paulo, ed. Globo, 1993
CARVALHO, Kildare Gonçalves *in "Direito Constitucional Didático"* Belo Horizonte, Del Rey, 1994

SOUZA, Carmen *in "O Estado Contemporâneo" - Revista Electrónica de Derecho Informático N.º 8, de março/1999* http://derecho.org/redi

DABIN, Jean *in "Doctrine Génerale de l'État"*, ed. Sirey, Paris 1939

JELLINEK, Georg *in "Teoría General Del Estado"*. Trad. de Fernando de Los Rios, Buenos Aires, Albatros, 1978

CAMPA, Ricardo *in "O Estado Contemporâneo"*, unidade IV: Relação Estado/Sociedade. A crise atual do Estado

SPENCER, Herbert *in "Essais de Politique"*, Paris, Alcan, 1920

Generación informatizada de sentencias en la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica

Informatización jurídica del Poder Judicial.

MS. Christian Hess Araya (Costa Rica)

RESUMEN:

Para administrar eficientemente la cuantiosa carga de trabajo que enfrenta la Sala Constitucional de Costa Rica, se ha introducido una serie de herramientas informáticas, entre las cuales destaca el denominado "Generador de sentencias" o "plantilla *sala.dot*". Este recurso automatiza los pasos repetitivos involucrados en la preparación de las resoluciones de fondo del tribunal, contribuyendo a acelerar el trabajo a la vez que se minimizan las posibilidades de error. Al mismo tiempo, se facilita la captura automatizada de las propiedades de los documentos, para efectos de su posterior sistematización e incorporación en las bases de datos de jurisprudencia constitucional.

INTRODUCCION

La Sala Constitucional de la Corte Suprema de Justicia de Costa Rica[1] fue creada en 1989, mediante reforma de los artículos 10 y 48 de la Constitución Política. Conforme a esos textos y a la Ley de la Jurisdicción Constitucional que en esa misma oportunidad fue promulgada también, le corresponde, en resumen:

- Garantizar, mediante los recursos de hábeas corpus y de amparo, los derechos y libertades consagrados por la Constitución Política y los derechos humanos reconocidos por el Derecho Internacional vigente en Costa Rica.

- Ejercer el control de la constitucionalidad de las normas de cualquier naturaleza y de los actos sujetos al Derecho Público, así como la conformidad del ordenamiento interno con el Derecho Internacional o Comunitario, mediante la acción de inconstitucionalidad y las consultas que le formulen la Asamblea Legislativa o las autoridades jurisdiccionales.

- Resolver los conflictos de competencia entre los Poderes del Estado, incluido el Tribunal Supremo de Elecciones, y los de competencia constitucional entre éstos y la Contraloría General de la República, las municipalidades, los entes descentralizados y las demás personas de Derecho Público.

- Conocer de los demás asuntos que la Constitución o la ley le atribuyan.

Como se nota, la misión fundamental de la Sala es garantizar la supremacía de las normas y principios constitucionales y del Derecho Internacional o Comunitario vigente en la República, su uniforme interpretación y aplicación, así como los derechos y libertades fundamentales consagrados en la Constitución o en los instrumentos internacionales de derechos humanos vigentes en Costa Rica.

Integran el tribunal siete magistrados propietarios y doce suplentes. Los asiste un cuerpo de asesores profesionales de tiempo completo (letrados), así como el correspondiente personal administrativo.

Desde su creación hace ya una década, la Sala ha debido enfrentar un volumen creciente de asuntos sometidos a su conocimiento. Esta realidad la reflejan los cuadros comparativos siguientes[2]:

---

[1] Véase su sitio web en www.abogados.or.cr/salaIV/index.html

[2] Fuente: Centro de Información de la Sala Constitucional.

Recursos de hábeas corpus	132
Recursos de amparo	187
Acciones de inconstitucionalidad	77
Consultas legislativas	3
Consultas judiciales	7
Conflictos de competencia; otros asuntos	1
Total	**407**

Tabla 1 - Ingreso de asuntos nuevos a la Sala Constitucional en 1989

Recursos de hábeas corpus	1073
Recursos de amparo	5743
Acciones de inconstitucionalidad	285
Consultas legislativas	48
Consultas judiciales	159
Conflictos de competencia; otros asuntos	1
Total	**7309**

Tabla 2 - Ingreso de asuntos nuevos en 1999, al 9/10/99

Se puede observar que el aumento en el ingreso de expedientes (teniendo en cuenta que las cifras para 1999 son sólo parciales) ha sido verdaderamente explosivo. En el último año, la Sala superó –por primera vez en su historia– la marca de diez mil sentencias dictadas en un año.

Evidentemente, este proceso ha obligado al tribunal a acudir a diversos mecanismos para administrar eficientemente la carga de trabajo y poder garantizar a los ciudadanos una justicia pronta y cumplida. Y, como se comprende, al reto de generar esa abundante producción sigue el desafío de clasificar y sistematizar la jurisprudencia resultante. Esto es especialmente urgente a la vista del hecho de que las sentencias de la Sala Constitucional son vinculantes *erga omnes*, lo cual obliga a dotar a la colectividad de medios efectivos para conocer sus alcances.

En síntesis, el proceso de elaboración de las resoluciones que dicta la Sala inicia con la preparación de un proyecto por parte del Magistrado que tiene a su cargo la instrucción de cada caso concreto, con el auxilio de sus letrados. Esta propuesta se somete al criterio del pleno de la Sala durante sus sesiones regulares, de adonde emerge una resolución final que luego deberá ser redactada en su versión definitiva, firmada y notificada a todos los interesados.

Una vez vertido el fallo, la sentencia pasa a un proceso de análisis a cargo del Centro de Información de la Sala, para su inclusión en las bases de datos correspondientes y publicación en la Revista Constitucional.[3]

A fin de allanar el proceso sumariamente descrito, se emplea en la Sala un conjunto de herramientas informáticas, entre las cuales figura la denominada "plantilla *sala.dot*" y que describiremos en lo que resta del presente trabajo.

[3] En el transcurso de este año se espera poner en funcionamiento el llamado "Sistema Costarricense de Información Jurídica", por medio del cual no sólo la jurisprudencia de la Sala sino también la entera legislación nacional y los pronunciamientos de los otros altos tribunales del país, serán accesibles por medio de Internet.

LA PLANTILLA *SALA.DOT*

El procesamiento de documentos en la Sala Constitucional se realiza mediante el paquete Microsoft Word.[4] Todas las sentencias presentan un formato estandarizado, fruto tanto de las exigencias legales como de la práctica del tribunal. A grandes rasgos, este esquema –similar al de muchos otros países de tradición jurídica romano germánica– distribuye el contenido de los fallos en tres grandes secciones continuas: a) la *parte fáctica*, contenida en una serie de "resultandos" que enumeran las circunstancias de hecho que dan pie a la sentencia; b) la *parte jurídica*, expresada en "considerandos" en los que la Sala discute el trasfondo jurídico del asunto; y, c) la *parte resolutiva* o "por tanto", en donde se expresa el fallo concreto vertido en el caso.

Preceden a esas secciones un encabezado que identifica el número del expediente; el número de resolución; el lugar, hora y fecha en que se dicta la sentencia y los datos de identificación del asunto. Las sigue el cuerpo de firmas de los magistrados que participaron en la decisión.

El hecho de que esta estructura esté completamente definida y que deba repetirse en cada resolución trae con facilidad a la mente la perspectiva de someterla a un proceso de automatización informatizada. Un procedimiento de este tipo tendría, por lo menos, los siguientes objetivos:

- Suprimir el tedio que para el operador jurídico supone seguir esos pasos mecánicos una y otra vez, permitiéndole concentrarse en el análisis jurídico del asunto.

- Minimizar la posibilidad de error al omitir elementos legalmente exigidos en el cuerpo de la sentencia.

- Uniformar la presentación de las resoluciones.

Como se verá, la herramienta actualmente utilizada en la Sala Constitucional no sólo asegura el cumplimiento de esas metas, sino que, además, permite lograr finalidades ulteriores de mucha importancia.

¿QUÉ ES *SALA.DOT?*

Sala.dot es una plantilla de Microsoft Word. Como se sabe, las plantillas de esa aplicación son archivos especiales, que contienen macros, autotextos, estilos y otros elementos asociados a la tarea para la cual se crean. En el caso de *sala.dot*, esas herramientas están destinadas al proceso de redacción de las sentencias de la Sala Constitucional. Sus componentes esenciales pueden ser divididos en dos: a) el "Generador de Sentencias"; y, b) las funciones adicionales de redacción e impresión.

La plantilla requiere del uso de la versión 97 o posterior de Word, debido a que las macros contenidas en ella están programadas en el lenguaje Visual Basic para Aplicaciones (VBA).

GENERADOR DE SENTENCIAS

Este es el elemento más complejo de la plantilla. Su propósito es crear rápidamente, a partir de los datos que le suple el usuario, un esqueleto de sentencia con todos los requerimientos legales. Al mismo tiempo, captura la información esencial del proyecto para su posterior lectura automatizada por el software empleado en la sistematización de la jurisprudencia de la Sala Constitucional.

El Generador de Sentencias (en lo sucesivo "GS") se lanza automáticamente cuando el usuario crea un nuevo documento en Microsoft Word, basado en la plantilla *sala.dot*. En este momento, despliega el cuadro de diálogo que se ilustra a continuación:

---

4 Marca registrada de Microsoft Corp. de Estados Unidos.

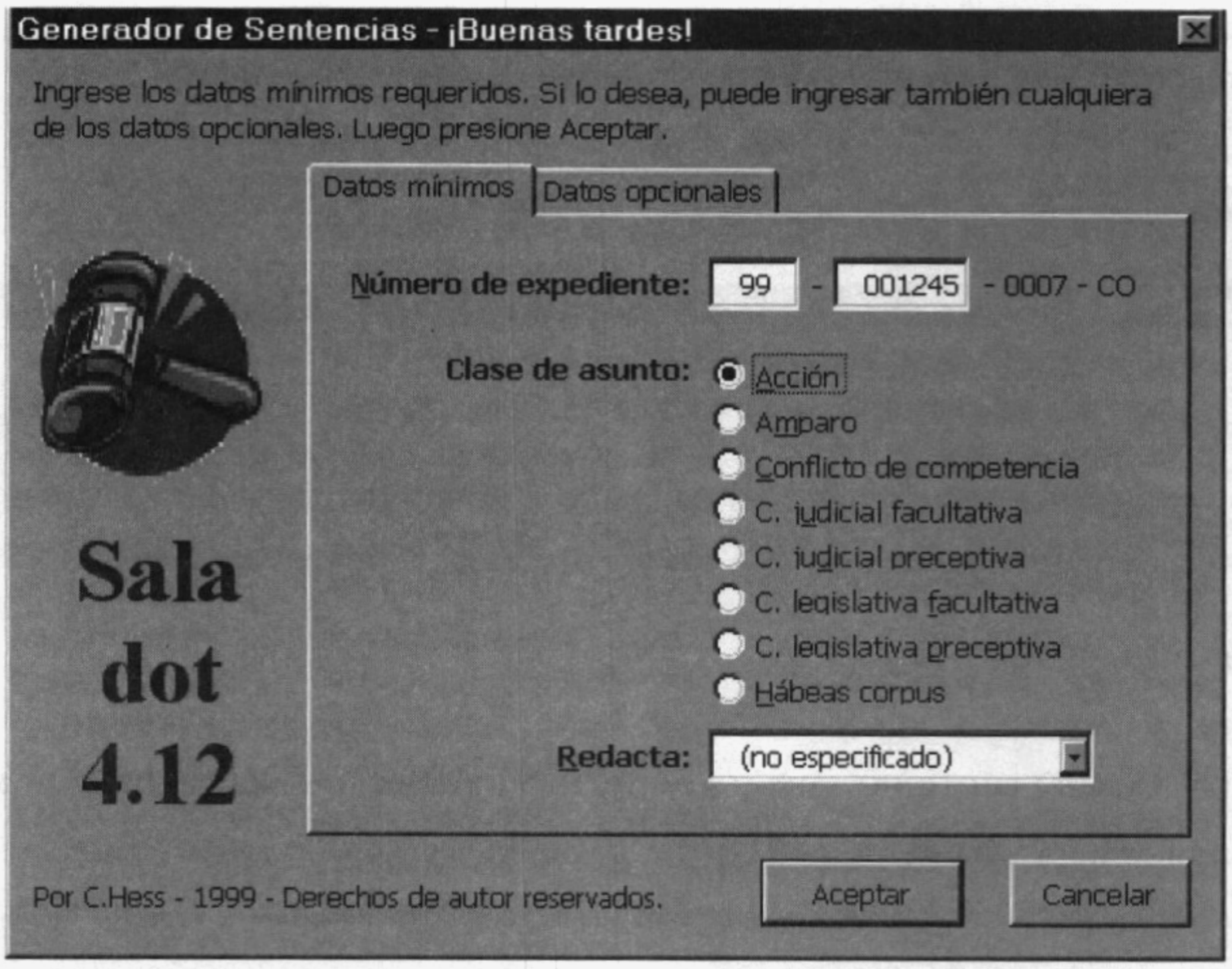


Figura 1 - Datos mínimos del Generador de Sentencias

En la ficha "Datos mínimos", el usuario especifica los datos obligatorios para la generación de un proyecto de sentencia (número de expediente, clase de asunto y apellidos del Magistrado redactor).

En la medida en que se disponga de esa información, es posible hacer uso además de los elementos de la ficha "Datos opcionales", que se muestra seguidamente:

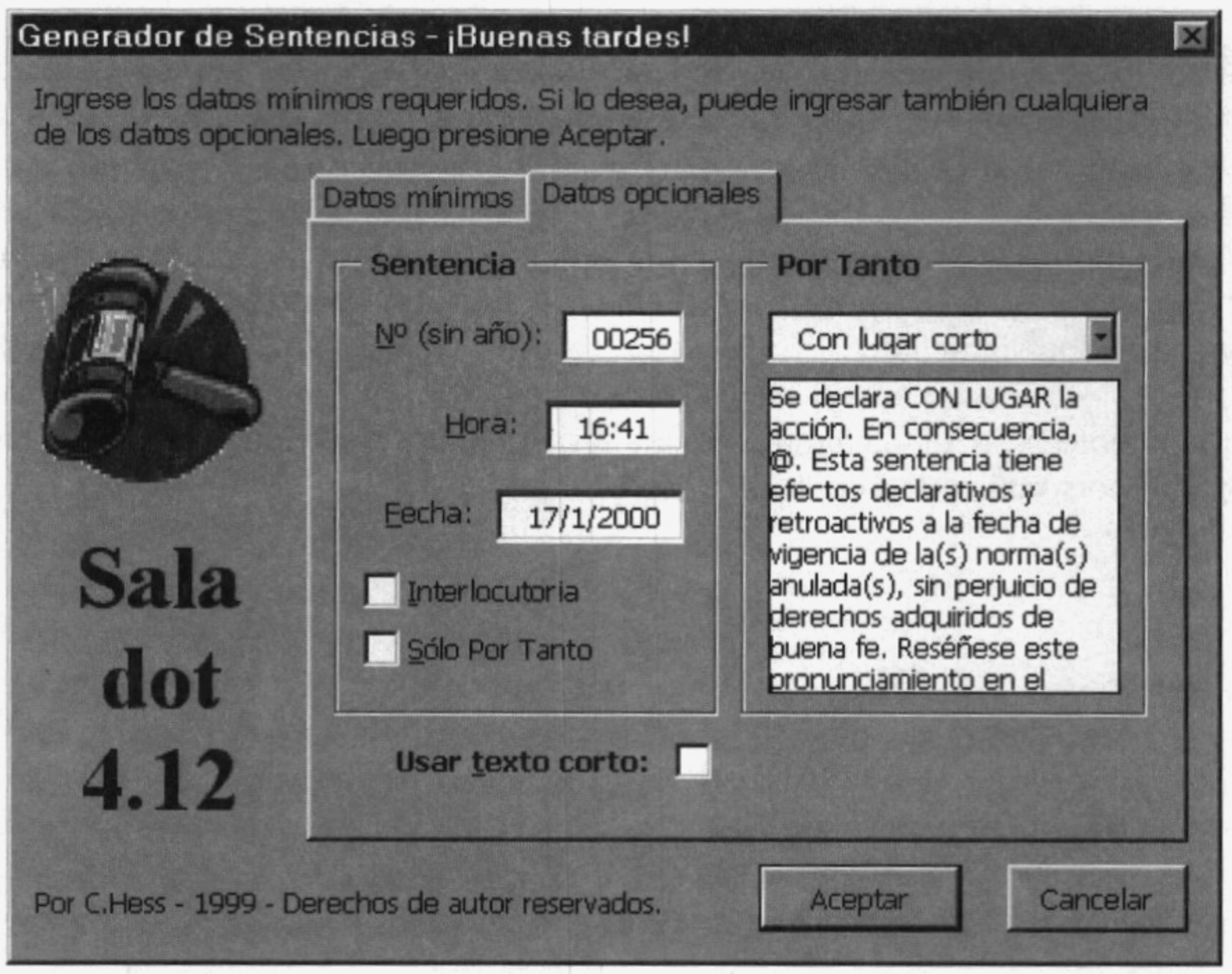
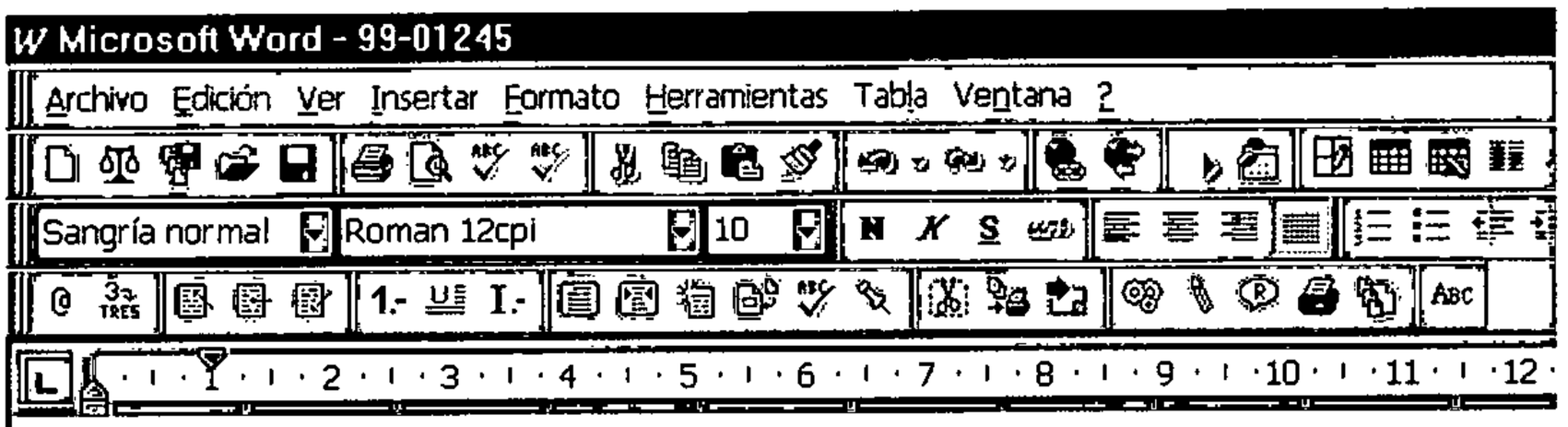


Figura 2 - Datos opcionales del GS

Desde luego, los datos de la sentencia sólo estarán disponibles si se trata de un asunto que ya ha sido resuelto por la Sala. El "por tanto" puede ser escogido de una lista de partes dispositivas que el tribunal ha venido estandarizando a través del tiempo y que, obviamente, más adelante será ajustado a las particulares características del caso.

Una vez pulsado el botón "Aceptar", el GS guarda el archivo y despliega seguidamente el resultado de su trabajo, similar al que se ilustra parcialmente aquí:


W Microsoft Word - 99-01245

Archivo Edición Ver Insertar Formato Herramientas Tabla Ventana ?

Sangría normal | Roman 12cpi | 10

Exp: 99-001245-0007-CO

Res: @-@

SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA. Sar

horas con @ minutos del @ de @ de @.-

Fin de sección protegida

Acción de inconstitucionalidad promovida por @, mayor, la cédula de identidad número @, vecino de @; contra @ también en el proceso @, @ y @, en representación de General de la República.

Figura 3 - Segmento del texto resultante

En el texto producido, se emplea el símbolo de la arroba (@) para denotar aquellos espacios en los que resta por agregar la información particular del caso o que no se conoce aún (como los datos de la sentencia, en tratándose de casos no resueltos todavía por la Sala).

Nótese en la figura anterior la presencia de una barra de herramientas complementaria (inmediatamente debajo de la barra de "Formato" de Word), por medio de la cual el usuario tiene acceso a las funciones adicionales que describiremos en la sección siguiente.

En adición al documento base, el GS almacena una serie de datos descriptivos de la sentencia, mediante una colección de propiedades personalizadas, como se observa aquí:

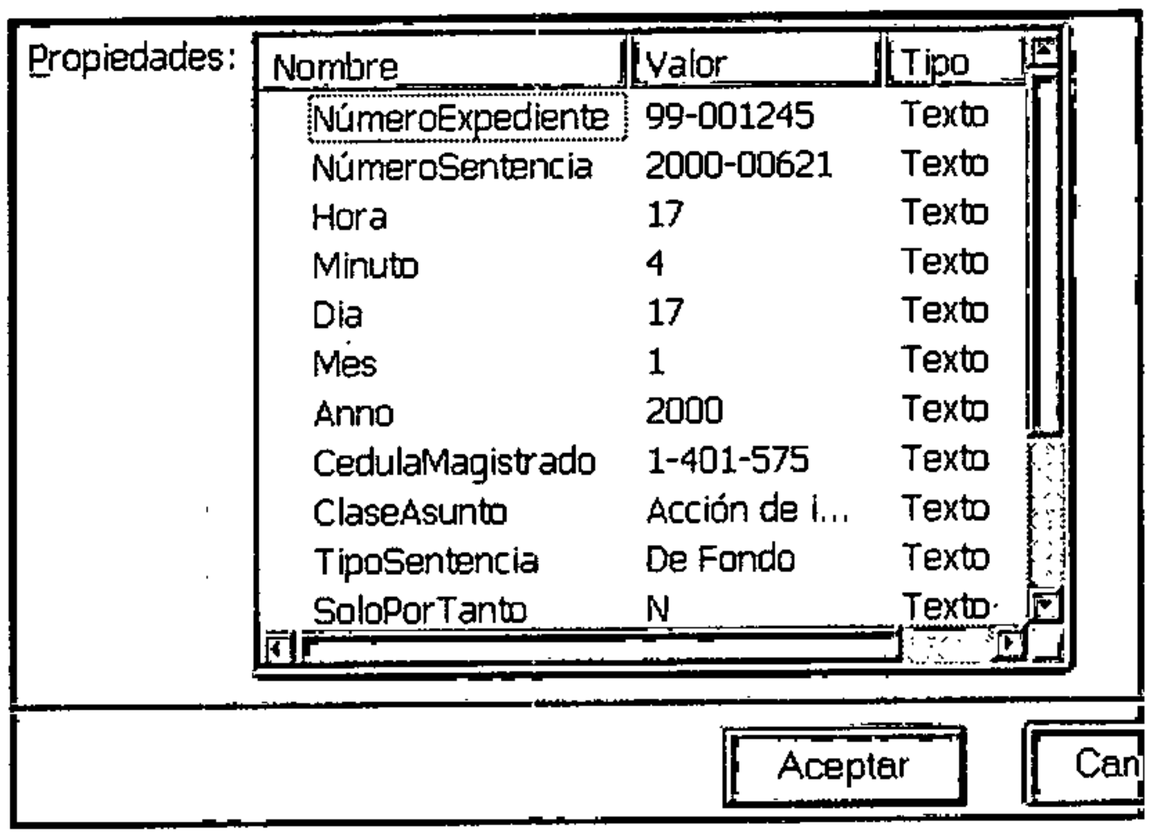


Figura 4 - Propiedades personalizadas del documento

Esta pequeña base de datos interna es empleada posteriormente por el programa de recopilación de jurisprudencia, durante la etapa de clasificación, como se ha mencionado ya.

FUNCIONES ADICIONALES

La utilidad de la plantilla *sala.dot* no se agota en la generación del borrador de la sentencia. La barra de herramientas (que se observa en la Figura 3 anterior) provee acceso a diversas funciones adicionales, de las que explicamos únicamente las principales:

1. Conversión de números a letras (por ejemplo, traduce "25" a "veinticinco"). Esto agiliza la redacción y elimina los errores que frecuentemente ocurren al realizar esta operación manualmente.

2. Navegación rápida a cada una de las tres secciones principales del documento (resultandos, considerandos, por tanto), lo cual es especialmente útil con sentencias largas.

3. Inserción de los llamados "textos usuales", que son citas jurídicas empleadas por la Sala para resolver asuntos repetitivos y frecuentes.

4. Modificación de las propiedades de la sentencia, a fin de guardar consistencia en el manejo de la información básica del documento.

5. Añadido de firmas de los magistrados participantes, guardando el orden correcto con que deben aparecer en la sentencia.

6. Impresión en limpio de la sentencia y de las cédulas de notificación. Durante el primer paso, se ejecuta también el duplicado del documento en la carpeta de red de la que posteriormente lo extraerá la aplicación de sistematización de jurisprudencia.

Para el adecuado desempeño de estas funciones, la plantilla conserva datos internamente acerca del estado del proyecto, advirtiendo al usuario sobre los posibles errores que la presión del trabajo podría propiciar de otro modo (por ejemplo, si intentara imprimir la versión en limpio de una sentencia a la que aun no se ha agregado firmas).

CONCLUSIÓN

La plantilla *sala.dot* es una herramienta valiosa para la más efectiva realización de la tarea de preparar y gestionar el número creciente de sentencias que la Sala Constitucional de Costa Rica debe dictar, en respuesta a una demanda masiva de justicia que ha experimentado durante los diez años de su existencia.

A pesar de ello, pensamos que hay amplio espacio para mejoras futuras. En particular, existe la meta de que, en el futuro próximo, sea posible extraer los datos esenciales de cada caso directamente del sistema de gestión,[5] logrando una mayor integración de las herramientas informáticas y una redacción más acelerada y precisa.

Sobre el autor

Christian Hess Araya, costarricense, es licenciado en Derecho y máster en Ciencias de la Computación e Informática, ambos grados de la Universidad de Costa Rica. Letrado de la Sala Constitucional de la Corte Suprema de Justicia y profesor de Derecho Informático en la Universidad de La Salle, en San José. Miembro de la Association for Computing Machinery (ACM).

Dirección postal: Apartado postal 239, Paseo de los Estudiantes. San José, 1002. Costa Rica. Teléfono: (506) 295-3902. Email: chess@poder-judicial.go.cr / chess@abogados.or.cr. Página web: www.geocities.com/SiliconValley/Circuit/1491/

[5] Ello no es posible actualmente debido a que el sistema de gestión corre en un ambiente de texto DOS que imposibilita un efectivo intercambio de datos entre aplicaciones.

Hacia una Democracia Digital: Propuestas de Aplicación

Carmen Milagros Velarde Koechlin* (Perú)

INTRODUCCION

Resulta innegable el auge que INTERNET ha tenido durante los últimos años como sistema de intercambio de información. Gran parte de esta información - de acceso gratuito por cierto - ha permitido el intercambio de ideas entre usuarios de todo el mundo, fomentando el desarrollo de investigaciones, actividades culturales, educativas, foros, etc.

El ciberespacio, sin duda alguna, se ha convertido, no en un medio de comunicación masiva como la radio, la televisión o la prensa, sino en una sociedad nueva donde los ámbitos geográficos no conocen fronteras. La expansión de INTERNET y la rapidez de sus comunicaciones, entonces, la convierten en una herramienta eficaz para la participación ciudadana, por lo que los Estados deberían considerar dentro de sus políticas el desarrollo de las nuevas tecnologías que sin duda alguna ayudarán al ciudadano al pleno ejercicio de sus derechos políticos, facilitando su intervención en las políticas de gobierno de su país.

El presente trabajo, tiene pues como objetivo llamar la atención de los Estados sobre la importancia del desarrollo de INTERNET como sociedad digital y la necesidad de fomentar su uso como mecanismo de participación ciudadana y, por tanto, promotor de una democracia digital. Para ello, hemos considerado dos aspectos importantes: El primero, referido al derecho de los ciudadanos de acceder a la red, lo que conlleva un deber del Estado de facilitar su acceso. La segunda parte, presenta la necesidad de contar con un Estado moderno, acorde al desarrollo de las nuevas tecnologías. Esperamos pues que los puntos aquí tratados, permitan el pronto desarrollo de una democracia digital.

1. EL DERECHO DE ACCESO A LA EED

El crecimiento de INTERNET y su posicionamiento como parte de la cultura y del desarrollo humano, siembra en cada una de las personas la necesidad de aprender, conocer y participar de la nueva sociedad digital. Por tanto, cada individuo tiene el derecho de acceder a la red, gozar de sus beneficios y atributos y utilizar sus herramientas en favor del progreso social. Este derecho debe ser reconocido por los diferentes Estados cuya labor es garantizar el respeto de los derechos ciudadanos. Es decir, asegurar el acceso de la población a la red.

A nuestro parecer, el derecho de acceso a la red se constituye como un derecho de tercera generación. Este derecho ha sido reconocido en la "Declaración de Derechos de INTERNET" aprobada en diciembre de 1999 por la Comisión de Redes Informática del Senado Español, también conocida como Comisión INTERNET, cuyo artículo I expresa:

"Todas las personas tienen el derecho fundamental de acceder libremente a la Red, sin discriminación de sexo, condición, característica físico-psíquicas, edad o lugar de residencia".

El acceso a la Red no puede estar condicionado, es libre y toda persona puede ejercerlo sin que éste le sea limitado. La situación social, económica o cultural de la persona no puede entonces constituirse como una barrera de inaccesibilidad a la red. La protección de este derecho corresponde al Estado, el que debe proteger y comprometer sus esfuerzos para el cumplimiento de este Derecho. La "Declaración de Derechos de INTERNET" resalta esta responsabilidad en su artículo III.

"Corresponde a los poderes públicos establecer las condiciones para que la libertad y la igualdad de las personas en la Red sean una realidad, eliminando los obstáculos que impidan el acceso de todos los ciudadanos a tal red y facilitando la participación de todos los españoles".

* Abogada de la Defensoría del Pueblo (Perú). Miembro del Estudio Velarde & Velarde Abogados. Fedataria Particular Juramentada en Informática por el Colegio de Abogados de Lima. Secretaria General del Cibertribunal Peruano. Miembro del Instituto Peruano de Comercio Electrónico.

Si bien el ámbito jurisdiccional de dicha Declaración se circunscribe a España, estimamos que la importancia de estos preceptos deben ser conocidos por los demás Estados, los que a través de una política de desarrollo de las nuevas tecnologías, asegurarán el acceso de sus habitantes a la Red.

Una de las barreras que limita el acceso a la red es el elevado costo que los usuarios pagan por el uso de la línea telefónica. En algunos países, tal precio se reduce mediante la utilización de una tarifa plana, es decir, el usuario realiza un único pago mensual que le permite acceder a la red cuantas veces lo requiera durante el mes. En el Perú, el costo de acceder a la red resulta elevado pues el usuario paga por cada minuto que se mantiene en línea. La aplicación de una tarifa plana permitiría a los usuarios un mayor período de navegación en la red, lo que incentivaría la búsqueda de información y por tanto, el desarrollo de investigaciones, foros sobre temas especializados, etc.

Por eso, ante tal situación, se ha fomentado el crecimiento de negocios denominados "cabinas INTERNET" en donde se cuenta con línea dedicada para acceder a la red. El valor de uso asciende a S/. 5.00 (US$1.5) por hora. Sin embargo, la aparición de estos negocios ha generado un aumento del uso de "software pirata" pues para ahorrar costos, los comercio no adquieren la licencia de uso de los programas, evadiendo el pago de los derechos de autor.

Asimismo, es menester resguardar el derecho de acceso a la red de los menores de edad, quienes no pueden estar ajenos a los avances tecnológicos, sin embargo, resulta indispensable construir un mecanismo que cuide la información proporcionada a los menores de edad en la red. Esta sugerencia no pretende censurar la información que es suministrada a través de la red, sino que intenta resguardar la salud mental de los menores de edad.

1.1. Luchar contra el analfabetismo electronico

El derecho de acceso a la red, como lo dijimos anteriormente, conlleva el deber por parte del Estado de garantizar a los ciudadanos y a la población en general, el conocimiento y uso de las nuevas tecnologías. Interesante resultaría que el Estado desarrolle políticas educativas que permitan a la población, aprender el manejo de la informática y el acceso a la red. Este programa sería aplicable a los diferentes grupos sociales existentes en cada país (comunidades campesinas, comunidades nativas, mujeres, niños, personas con discapacidad, etc.)

El Estado debe velar porque no existan analfabetos electrónicos. Dado que todas las personas tienen derecho a la educación, se entiende que cada individuo debe acceder a una enseñanza básica, la que evidentemente, incluirá el conocimiento de la informática.

Para complementar este programa educativo, resultaría útil el desarrollo de una política de implementación de cabinas de INTERNET en las bibliotecas públicas, municipios y otras entidades públicas. Dichas cabinas estarían habilitadas con software legalmente adquiridos y facilitaría el acceso de la comunidad a la información de las entidades estatales.

Evidentemente, mientras más gente ingrese a la red, habrá un mayor intercambio de ideas e información. Pero para lograr tal tarea, es necesario que cada individuo conozca el manejo de la red. Por tanto, vencer el analfabetismo electrónico es una labor ardua pero necesaria, pues no se puede limitar el ingreso a la red a tan sólo un grupo de ciudadanos ya que ello sería colocar la información que circula en INTERNET en manos de un grupo social.

Por ello, estimamos indispensable que en los colegios se enseñar cursos de informática y sobre todo, cursos de acceso a la red.

1.2. El acceso de las personas con discapacidad

El derecho de acceso corresponde a todas las personas y no puede limitarse por su condición o características físicas o psíquicas, pues ello evidenciaría un acto de discriminación. Por ello, es necesario que el Estado tenga en cuenta, para una adecuada protección del derecho de acceso a la red, la existencia de grupos vulnerables como: comunidades campesinas, comunidades nativas, mujeres, personas con discapacidad, etc.

A nuestro parecer, uno de los grupos más vulnerables es el de personas con discapacidad, quienes, de acuerdo al tipo de discapacidad que presentan, se encuentran con dificultades para acceder al uso de la informática pero sobre todo, para acceder al uso de INTERNET.

Por ejemplo, las personas con discapacidad visual, sean personas invidentes o de baja visión, tienen grandes inconvenientes parea acceder al uso de la informática. Si bien pueden memorizar el teclado para escribir sus documentos, requieren de una tercera persona que los corrija para evitar las faltas ortográficas, etc. Asimismo, no pueden laborar con la barra de herramientas de los diversos programas. En INTERNET, evidentemente, no pueden leer la información contenida ni gozar de las imágenes.

De igual modo, las personas con cuadraplejia que no pueden utilizar sus manos no pueden utilizar el teclado de la computadora o el mouse, por lo que requieren de un tercero que los apoye en la búsqueda de información a través de INTERNET.

Para ellos, existen programas como el "Via Voice" que permiten a las personas con discapacidad, dictar a la computadora a través de un micrófono. De igual modo, existen programas que permiten a las personas con discapacidad visual conocer la información de INTERNET al leerles la información encontrada. Sería interesante que los centros educativos y las universidades, así como municipios y bibliotecas públicas, tengan un mínomo de terminales que permitan el acceso de las personas con discapacidad al uso de la informática.

2. LA MODERNIZACION DEL ESTADO A TRAVES DE LA DEMOCRACIA DIGITAL

Contar con un Estado moderno significa hoy en día, gozar de un Estado que desarrolle las nuevas tecnologías como herramienta de comunicación con sus ciudadanos. Por ello, consideramos necesario tomar en cuenta los siguientes puntos.

2.1. El acceso a la información de las entidades Públicas

Es recomendable que las entidades públicas cuenten con una página web que transmita información sobre sus actividades a los ciudadanos. Muchas veces resulta tedioso apersonarse a una institución pública para conocerla, por lo que INTERNET se convierte en una vía de fácil acceso hacia ellas. Estas páginas web brindarían la información indispensable a los ciudadanos, además, sería interesante que cuenten con foros de discusión para escuchar las opiniones de la población. También sería importante la creación de una lista de suscripción con temas de interés que transmita con mayor facilidad los avances de las instituciones del Estado.

Más interesante resultaría que dichas páginas web permitan a los ciudadanos realizar operaciones como pagos de tasas, aranceles y otros tributos, así como solicitar información de las instituciones.

2.2. El desarrollo de los derechos políticos

INTERNET permite a los ciudadanos desarrollar sus derechos políticos. Por ejemplo, los partidos y agrupaciones a través de una página web pueden informar a la población sobre sus planes de gobierno y fines de su organización. La red, evidentemente, ha servido para apoyar el desarrollo de los derechos políticos, sobre todo, en épocas electorales. Por ejemplo, algunos partidos y agrupaciones políticas han utilizado INTERNET para su publicidad. Recordemos que en el Perú, el pasado 4 de julio de 1999, se realizaron las elecciones municipales complementarias. Un candidato a la alcaldía utilizó el correo electrónico para enviar a los ciudadanos una carta exhortando a votar por él. Quienes no participaban en estas elecciones recibieron sin embargo dicha publicidad. Esta situación, sin embargo, cuenta también con situaciones desfavorables como el hecho de recibir una propaganda de un candidato que no es de mi preferencia y que en todo caso acumula espacio en mi casilla de correo. Esta situación debe ser tomada en cuenta para mantener un equilibrio en el uso de la red.

2.3. El derecho de iniciativa legislativa: el parlamento virtual

Una de las entidades más importante para los ciudadanos es el Parlamento, ya que como Poder Legislativo, tiene la capacidad de decidir la creación de leyes y medidas que regularán la vida en sociedad y sus diversos aspectos.

Resultaría muy estimulante para los ciudadanos que cada Parlamento constituyera su propia página web. sin embargo, dicha página no debe ser tan sólo una mera nota informativa de los representantes del Congreso o de las comisiones de trabajo, sino que deben convertirse en un "Parlamento Virtual" que permita a los ciudadanos participar en el análisis de los problemas sociales, económicos, etc. Dichos sitios web, para constituirse como fuente de participación ciudadana, contaría con foros de discusión sobre los temas de debate en el Congreso, lo que permitiría al público no especializado seguir esta discusión, empapándose de la materia. Por eso, a nuestro parecer, el Parlamento Virtual debe constituirse como medio de comunicación entre las autoridades parlamentarias y los ciudadanos.

A través de tal mecanismo - el Parlamento Virtual - se podría someter los proyectos de Ley que posteriormente serían debatidos en el Congreso y a través de una consulta popular, podría conocerse la opinión de la ciudadanía. A través del Parlamento Virtual los ciudadanos podrían votar por una determinada propuesta y esta decisión podría ser comparada luego con la votación hecha por los congresistas, lo que permitiría saber si efectivamente los legisladores están representando la voluntad popular.

De aplicarse esta propuesta, es necesario recordar la necesidad de eliminar el analfabetismo electrónico ya que mayor cantidad de ciudadanos tendrían la necesidad de acceder a la red para ser "escuchados". El Parlamento Virtual fomentaría la participación de las amas de casa, estudiantes universitarios no sólo de las Facultades de Derecho sino de otras carreras universitarias, etc.

Es necesario acercar la información del Estado a los ciudadanos. Por ejemplo, Estados unidos, a través de su Vice-Presidente, Al Gore, anunció la puesta en marcha de dos proyectos: uno primero denominado directiva E-Government que pretende acercar toda la información gubernamental a los ciudadanos a través de INTERNET. El segundo es la directiva E-Society que busca mejorar la vida y educación de los ciudadanos mediante el uso de la red.

Actualmente el en Perú, el Poder Legislativo ha puesto en marcha el denominado "Parlamento Virtual", que permite a los ciudadanos inscribirse y recibir semanalmente una relación de los Proyectos de Ley presentados por los congresistas. Asimismo, diariamente, se informa a los ciudadanos inscritos sobre las noticias más resaltantes a nivel nacional e internacional. Recibidos los Proyectos de Ley, los ciudadanos pueden enviar sus opiniones. La página web del Congreso de la República del Perú, incluso, proporciona la dirección electrónica de los congresistas para que los ciudadanos puedan comunicarse con ellos. Sin embargo, este mecanismo debe repotenciarse, es decir, el ciudadano debe sentirse escuchado y por tanto, recibir una respuesta por parte de las autoridades luego de enviar un email. Si las opiniones emitidas electrónicamente por los ciudadanos no obtienen una respuesta, entonces, el Parlamento Virtual no estaría cumpliendo su función.

2.4. El derecho de sufragio: voto por Internet

Otra de las propuestas para desarrollar un Estado moderno es desarrollar la aplicación del voto por INTERNET. Es decir, los ciudadanos sufragaría a través de la red, evitándose el acudir a locales de votación, hacer colas. La información recibida sería procesada con ayuda de un software que emitirá los resultados en pocas horas. Claro está que para desarrollar tal sistema, es necesario garantizar que el voto será seguro, por tanto, podrían asegurarse la emisión del voto a través del uso de firmas digitales por cada ciudadano. Sin embargo, habría que sortear otros obstáculos como la existencia de hackers que podrían alterar los resultados de las votaciones.

En el caso del uso de la firma digital, cierto es que se corre el riesgo de que ésta sea robada y utilizada por un tercero que emita el voto por mí, perdiendo mi derecho a reclamar. Por ello, tal vez, la biometría sea una salida interesante, pues en el padrón electoral figuraría nuestra huella digital. El votante deberá escanear su huella, que de coincidir, el sistema admitiría el voto como válido.

Hay legislaciones como la española que permiten el voto por correo, entonces, por qué no permitir el voto a través de INTERNET. Ello facilitaría el voto de los extranjeros o también facilitaría el voto de los votantes que el mismo día de la votación se enferman y por tanto no pueden acudir al centro de votaciones. Ellos no deberían perder su derecho de sufragio y más aún, con la consecuencia de que algunas legislaciones - como la peruana - imponen el pago de una multa por no votar. De igual modo, personas con discapacidad que no pueden salir de sus hogares o cuyos locales de votación no resultan accesibles, se verían favorecidas con este sistema que les permitirá votar desde su casa a través de INTERNET. Asimismo, resultaría adecuado colocar en los hospitales, módulos o cabinas que permitan a los pacientes votar.

Claro está que el sistema admitirá a aquellos inscritos en el padrón electoral por tanto debe alimentarse el sistema o el programa con una base de datos de los electores, lo que evitaría que los menores de edad votaran. Luego de haber votado el sistema devolverá un mensaje que indique haber recibido el voto, algo similar al mensaje emitido luego de suscribirnos a una lista.

Las votaciones electrónicas pueden ser un complemento de las votaciones tradicionales.

Actualmente, se ha utilizado el voto electrónico en países como Bélgica, francia u Holanda. En Sudamérica, Brasil utilizó el sistema de votación electrónica en las pasadas votaciones del 4 de octubre de 1999. Sin embargo, este sistema labora con la colocación de urnas electrónicas en los centros de votación. Estos módulos son similares a los cajeros automáticos y el beneficio que brinda es que evita los votos nulos y facilita el conteo de los votos.

El voto electrónico ayuda a terminar con un sistema manual que resulta lento y burocrático e inclusive caro, pues facilita el llenado de las actas, y el conteo rápido de los votos. Ya no tendría que contarse con varios miembros en la mesa electoral, bastará con una ó dos personas. Invertir en este sistema resulta poco caro si se toma en cuenta que la adquisición del equipo y módulos se hace por una única vez ya que luego sólo habría que brindarles mantenimiento.

CONCLUSIONES

- Todas las personas tienen el derecho de acceder a la red, por lo que el estado debe garantizar el cumplimiento efectivo de este derecho.

- Es necesario que el estado instaure una política de desarrollo de las nuevas tecnologías, así como una política educativa que contemple el aprendizaje de INTERNET por los alumnos desde su minoría de edad. Dicha política estará dirigida a la erradicación del analfabetismo electrónico, otorgándose prioridad a los grupos vulnerables como comunidades campesinas, comunidades nativas, personas con discapacidad, amas de casa, etc.

- Las personas con discapacidad resultan parte del grupo vulnerables, por lo que el desarrollo de las nuevas tecnologías debe contemplar software especiales que les permitan acceder no sólo a INTERNET, sino al uso de la informática.

- El estado debe aprovechar los recursos que brinda la red de redes para comunicarse con los ciudadanos, por lo que es necesario implementar una política de acercamiento a los ciudadanos a través de la red. Indispensable resulta que las instituciones del estado cuenten con una página web que permita al ciudadano conocer sus funciones y realizar sus operaciones a través de INTERNET.

- El desarrollo de un Parlamento Virtual apoyaría la ejecución de los derechos políticos y de participación ciudadana que compete a los miembros de una sociedad.

- El desarrollo del voto electrónico facilitaría los procesos de sufragio en la medida que permite contar con elecciones menos caras, más rápidas y certeras con la eliminación de votos nulos.

Razionalización Informática para la Legislación

A propósito del Manual del Digesto Jurídico Argentino

Antonio A. Martino (Italia)
martino@dsp.unipi.it

Una de las características que ha atravesado el siglo que termina es la escrupulosidad con la cual se han estudiado, analizado, perfeccionado y utilizado todas las técnicas y medios posibles de la lucha por el poder. Es mas parecería que la ciencia política moderna no se ocupara de otra cosa. En cambio la lucha por el poder es solo una cara de la medalla, la otra es el gobierno.

Se podrida decir que los politologos se ocupan demasiado del conflicto y que los abogados se ocupan (con ojeras) de lo que se da como producto. Se podría decir, pero no lo diremos pues es una exageración. Afortunadamente en uno y otro campo ha habido tentavas serias de ocuparse de esa caja negra que produce el derecho una vez conquistado el gobierno. Y no me refiero solo a los magníficos tratados de Derecho Constitucional que el siglo ha producido.

En un ámbito mas modesto, pero mas inquieto por el fermento tecnológico, otros estudios de Teoría General del Derecho y en la ultima parte del siglo de Informática Juridica se han ocupado de este tema: hay criterios de racionalidad mínima para el gobierno? [1]

Los desarrollos de la lógica normativa[2] de la teoría general de sistemas [3] y de la acción racional [4] han desarrollado una conciencia de las políticas publicas que supera las etapas del férreo dirigismo para un desarrollo sostenible.

Entre los muchos temas que el siglo ha tratado hay uno que merece particular atención: la racionalidad de la documentación. Lo digo en este modo poco altisonante para que se vea todo el efecto que comporta.

Si hay lucha por el poder hay también lucha entre poderes. Una de las formas de no llegar a la guerra es establecer las reglas del juego, sabiendo bien que quien las establece generalmente no tiene la venda que cubre su colocacion real en el nuevo campo de juego [5] Pero nadie puede evitar que, aun dictadas las reglas se luche por las interpretaciones posibles[6] Hay lucha entre fuentes del derecho.

Cuando el derecho era típicamente doctrina, Justiniano reordeno toda la serie de pareceres en una obra ciclópea llamada Digesto. El final del siglo nos encuentra abocados a una tarea parecida si bien limitada o otra fuente: la ley, que ha terminado por prevalecer (si bien come se dice en musica "ma non troppo").

A los entusiasmos de la codificación siguieron los entusiasmos de la muerte de la codificación y no es de hoy la diatriba entre A.F. J Thibaut y F.C. Savigny . Este ultimo concluye con una expresión que aun hoy es actual: " los puntos en los cuales mi opion coincide con las de los defensores de un código y los punto en los cuales divergen. Nuestro objetivo es el mismo: queremos el fundamente de un derecho seguro, seguro de la injerencia y del arbitrio de los las ideas injustas; también queremos la comunidad de las naciones y la concentración de su actividad científica sobre el mismo objeto. Para alcanzar tal objeto, ellos piden un código, que daría empero al suspirada unidad solo a la mitad de Alemania e insolaría en

---

[1] O lo que Norberto Bobbio, llamaba en modo mas clasico en sus clases de Turin en 1973 "las reglas del buen gobierno"

[2] G H von Wright, Deontic logic, Mind, 1951

[3] von Wartanfli

[4] K. Arrow, Individual values and public choice, 1957

[5] Rolls, The Theory of Justice, 1971

[6] Solo San Francisco prohibio expresamente que se interpretaran sus Regulae, y se desato una de las guerras mas cruentas del Medioevo: la de los Minoritas.

cambio a la otra mitad mas netamente que antes. Yo veo el medio justo en una ciencia jurídica en progreso orgánico que pueda ser común a toda la nación... "[7]. Hoy con la globalizacion, hablaríamos de comunidad mundial.

Ya en una celebre resolución del 25 de marzo de 1995 la OCED[8] ha prevenido a los gobiernos de los piases que piden créditos a los mas ricos (este es el club de la OCED) que estos estaran subordinados, en el futuro, a que tengan la legislación en orden. Y dice además n que consiste este orden en diez proposiciones que constituyen el

---

7 F.C. Savigny, *La vocacion de nuestro tiempo para la legislacion y la jurisprudencia (doctrina) Digo "doctrina" pues en aleman es Wesenchafl aunque* los angloamericanos impusieron la nocion de Jurisprudece (como se ve tambien guerras academicas), Heidelberg 1814

8 Recommendation of the Council of the OECD:

Appendix 1: The OECD Reference Checklist for

Regulatory Decision-Making

Government performance is under pressure. Systems of governance are adapting to global transformation involving more cooperation between countries, intensified economic competition, and new technologies. Budget deficits and economic constraints must be managed even as citizens demand more action to deal with emerging social and environmental issues. As a result, public sectors must learn to do more with less, differently and better, *as the OECD Public Management Committee has noted. Governments must find effective ways to make responsive policy* decisions and to identify the right mix of

instruments and incentives to implement them.

The OECD Reference Checklist for Regulatory Decision-making responds to the need to develop and implement better

regulations. It contains ten questions about regulatory decisions that can be applied at all levels of decision- and

policy-making. These questions reflect principles of good decision-making that are used in OECD countries to improve the effectiveness and efficiency of government regulation by upgrading the legal and factual basis for regulations, clarifying options, assisting officials in reaching better decisions, establishing more orderly and predictable decision processes, identifying existing regulations that are outdated or unnecessary, and making government actions more transparent. The Checklist, however, cannot stand alone — it must be applied within a broader regulatory management system that includes elements such as information collection and analysis, consultation processes, and systematic evaluation of existing regulations.

Question No. 1

Is the problem correctly defined?

The problem to be solved should be precisely stated, giving clear evidence of its nature and magnitude, and explaining why it has arisen (identifying the incentives of affected entities).

Question No. 2

Is government action justified?

Government intervention should be based on clear evidence that government action is justified, given the nature of the problem, the likely benefits and costs of action (based on a realistic assessment of government effectiveness), and alternative mechanisms for addressing the problem.

Question No. 3

Is regulation the best form of government action?

Regulators should carry out, early in the regulatory process, an informed comparison of a variety of regulatory and non-regulatory policy instruments, considering relevant issues such as costs, benefits, distributional effects, and administrative requirements.

Question No. 4

Is there a legal basis for regulation?

Regulatory processes should be structured so that all regulatory decisions rigorously respect the "rule of law"; that is, responsibility should be explicit for ensuring that all regulations are authorised by higher- level regulations and consistent with treaty obligations, and comply with relevant legal principles such as certainty, proportionality, and applicable procedural requirements.

esqueleto de cualquier checklist [9]. Lo curioso es que el impulso viene de los economistas que hay descubierto que la economía no es "una variable independiente" y que depende justamente de la estabilidad juridica [la cual obviamente depende de la estabilidad política].

En este marco deben ser vistos todos los esfuerzos que en muchos paises se estan realizando para racionalizar la legislacion, obviamente en busqueda de ese oasis legislativo que es la legislacion en vigor.[10]

Muchas obras tecnicas fueron realizadas en este campo y lo primero que descubrimos fue que no era tanto el numero de las leyes lo que traía confusión sino su falta de coordinamiento. Se habla de la inflacion legislativa como el mal de esta segunda parte del siglo, donde los politicos aprendieron que se puede conceder cualquier prebenda, ventaja, derecho o lo que fuere a pacto de no colocar quien (o quienes) son los sujetos obligados. Nació la concepción de Jauja, y los niños (probablemente en reacción a un pasado culposo) descubrieron tener muchos derechos[11]

Question No. 5

What is the appropriate level (or levels) of government for this action?
Regulators should choose the most appropriate level of government to take action, or, if multiple levels are involved, should design effective systems of coordination between levels of government.

[Question No. 6

Do the benefits of regulation justify the costs?
Regulators should estimate the total expected costs and benefits of each regulatory proposal and of feasible alternatives, and should make the estimates available in accessible format to decision-makers. The costs of government action should be justified by its benefits before action is taken.

Question No. 7

Is the distribution of effects across society transparent?
To the extent that distributive and equity values are affected by government intervention, regulators should make transparent the distribution of regulatory costs and benefits across social groups.

Question No. 8

Is the regulation clear, consistent, comprehensible, and accessible to users?
Regulators should assess whether rules will be understood by likely users, and to that end should take steps to ensure that the text and structure of rules are as clear as possible.

Question No. 9
Have all interested parties had the opportunity to present their views?
Regulations should be developed in an open and transparent fashion, with appropriate procedures for effective and timely input from interested parties such as affected businesses and trade unions, other interest groups, or other levels of government.

Question No. 10

How will compliance be achieved?

Regulators should assess the incentives and institutions through which the regulation will take effect, and should design responsive implementation strategies that make the best use of them.

9 Una checklist es una especie de recordatorio esencial que por ejemplo usan los aviadores antes de despegar vuelo.
11 Por cierto los ninos de los paises de la OCDE

Contaminacion legislativa, es el termino que utilicé en varias obras a partir de 1975[12] y que ha tenido una cierta aceptacion en doctrina. La contaminacion da cuenta no solo del aumento de uno de los elementos sino sustancialmente de la imposibilidad de eliminar la basura, que en materia legislativa son las derogaciones.

Encarar la revision y reordenación de la legislacion en vigor no es pequeña cosa y por lo tanto vale la pena saber qué se esta haciendo en este campo y como.

La Republica Argentina tiene el raro privilegio de haber enfocado de manera general y de frente el tema. No es un caso: grandes juristas argentinos han descollado en estos temas desde Alfredo Colmo, *Tecnica Legislativa* en la Argentina se ha desarrollado una de las escuelas de logica normativa mas conocida en el mundo [13], en particular el desarrollo de la informática jurídica permitió fundar en 1981 el SAIJ[14]. Y existen centros de estudios especiales de la legislación[15] Pero, honor a los políticos, en 1997 se dicto una ley la 24967 que estableció los pasos y criterios por los cuales se puso en marcha el Digesto argentino. La ley 24967 estableció el reordenamiento de toda la legislación argentina Para hacerlo es necesario utilizar un criterio uniforme para renumerar y reordenar las leyes precedentes así como utilizarlo en la redacción de las leyes futuras.

La ley prevee que se revisen las 25 mil leyes existentes hasta la fecha y los respectivos decretos y se los reordene en 25 categorías que con las letras del abecedario español (excluyendo las dobles) fueron identificadas. Cualquier criterio de clasificación es arbitrario y los sectores jurídicos que fueron indicados seran objeto de muchas discusiones y deslindamientos. Pero el derecho argentino tiene 25 sectores indicados por ley.

La ley prevee una comisión de 25 eminentes juristas (que esta por nombrarse) dice la ley "para redactar" el Digesto, en verdad es para revisar la realización de un Digesto que ya ha comenzado con un vasto equipo de juristas dirigidos por Atilio Alterini,[16]. Para hacer esta inmensa obra se requiere un plano o manual y este me fue encargado[17] por la Facultad de Derecho de la UBA la cual conjuntamente con las revistas La Ley, Jurisprudencia Argentina, El Derecho ganaron la licitación para realizar la obra.

A ojos de buen cubero, de las 25 000 leyes, mas de mil están expresamente abrogadas y mas de 14 000 no son computables como leyes en vigor o porque nacieron para casos individuales y se agotaron o porque su objeto esta precluido u obsoleto, o cayo en desuso. Probablemente las aun en vigor no lleguen a diez mil y de ellas menos de tres mil deben ser originarias y el resto modificaciones. Esta estima "a ojo" puede recibir lo que Hegel llamaba "las duras replicas de la historia", por lo tanto deben ser consideradas como lo que son: una simple estima. Pero aunque cambien los números no cambia la sustancia: una parte importante del orden jurídico argentino ira al lugar que ocupa solo que solapadamente: el derecho histórico, pues dado que las relaciones juridicas no se realizan necesariamente en el presente, sera menester dejar el derecho histórico para saber qué ley regia una cierta situación.

El Manual del Digesto propuso los temas clásicos de la legislación, y en particular un añoso tema que hemos discutido muchas veces en Sadaf[18]: hasta cuando una regla debe mandar, cuanto debe preveer las excepciones. El tema es muy complejo y desde el punto de vista filosófico tiene desarrollos importantes variantes desde el imperativo categorico kantiano (ninguna excepción) hasta la posición mas extremista de David Ross[19] con su ética "prima facie" donde los deberes y los derechos dependen de la información que se tenga, con esta información el deber que se impone es este, pero podria variar con el variar de datos de hecho y no solo de normas.

---

12 Buenos Aires, 1927.

13 Baste nombrar el ya clasico Normative Systems de C.E. Alchourron y E. Bulygin

14

15 Como el Master en Ciencia de la Legislacion que se dicta en la Universidad del Salvador, con la colaboracion de la Universidad de Pisa.

16 coordinados por Daniel Ricardo Altmark y que cuenta en su parte tecnica la direccion de Ramon J. Brenna

17 Equipo de trabajo del Manual: Director: Prof. Antonio A. Martino, Analistas: Dr. Pietro Mercatali y Dr. Carlo Biagioli. Lingüistas: Dra. Manuela Sassi, Dr. Roberto Brocchini. Juristas: Dra. Maria Cristina Pagano y Dra. Silvia Pfarherr.

18 Sociedad Argentina de Analisis Filosofico

19 David Ross, Fundation o/ Etbics, Oxford University Press, London, 1930

Sabemos que la descripción de Ross es mas cercana a como efectivamente se comportan los hombres que la de Kant. No obstante y porque la maxima kantiana tiene una funcion pedagogica, nuestras reglas (las hemos llamado reglas para asimilarlas a las reglas tecnicas) son concebidas en modo imperativo, escueto y con cuentagotas: 71 reglas y 25 definiciones.

El objeto principal del manual es, la vocación de constituir un instrumento util para el reordenamiento de las leyes existentes y al mismo tiempo para continuar con esta misma técnica en la redacción de las leyes futuras. presentar las reglas (pocas),casi como inevitables, en el fondo se trata de una recomendación técnica que los legisladores dirán si y cuanto están dispuestos a seguir. La pena por no seguir estas reglas es la contaminación legislativa. En el fondo creemos en la que hay que revertir la vieja idea que el legislador debe legislar todo lo que puede. Hoy la tendencia, es al revés, solo en caso de justificada necesidad se habrá de legislar, recordando que legislar es modificar el actual orden en vigor [20]

Al Manual le ha seguido un CD para poderlo visualizar como un libro en forma di hipertexto, esto es un texto enorme que tiene a su vez referencia que llevan a profundizar partes de ese texto. *Nec novum sub solem*. La idea de hipertexto, solo que limitada a dos dimensiones por las razones físicas que impone el papel había sido desarrollada en el campo jurídico sea en el mundo judío que en las glosas del Digesto [21]

El Manual contiene algunos ejemplos tomados de las leyes argentinas y algunas fórmulas de aplicación de las reglas. Esta acompañado por una check list, esto es una lista de recomendaciones esenciales al redactor (o reordenador legislativo) así como los en los aviones los pilotos están obligados a verificar una lista antes de decolar. [22]

Nuestra esperanza es recibir criticas y que al final pueda obtenerse algo así como un standard de redacción de leyes. Este seria una enorme contribución de la informatica para con la legislacion.

[20] Y esto resulta mas patente en los capítulos que tratan del arte de «gobierno»: el soberano ideal es aquell que gobierna sin gobernar es deci> sin intervenir respetando el libre curso de los acontecimientos. Entonces la sociedad de los hombres se ordenar por si misma espontáneamente. La intervención del gobernante no es sino una piedra lanzada que enturbia y descompone la tranquila igualdad de las aguas del estanque. LAO ZI [EL LIBRO DEL TAO], 1983, EDICIONES ALFAGUARA, S. A. Madrid.

[21]



Primera Pagina del Talmud (Soncino) Publicado en 1483 por el Seminario Teológico Judío.

[22] Obviamente hemos seguido con atencion la redaccion de la check list de la OCDE

Estudio sobre la Viabilidad Jurídica de un Sistema de Transmisión Telemática de Documentos Administrativos entre Administraciones Públicas

Beatriz Verdera Izquierdo (España)
Profesora Ayudante de Derecho Civil
Universidad de las Islas Baleares

I.- INTRODUCCION. OBJETIVO DEL ESTUDIO

El presente estudio jurídico preliminar se sitúa dentro de un proyecto con el que se pretende establecer un sistema de comunicación telemática entre el Ayuntamiento de Palma de Mallorca y la Comunidad Autónoma de las Islas Baleares. La finalidad de este proyecto consiste en que el Ayuntamiento de Palma pueda remitir los documentos jurídico-administrativos por él creados y que han de ser publicados en el Boletín Oficial de la Comunidad Autónoma de las Islas Baleares (BOCAIB), al Servicio de publicación de dicho boletín oficial dependiente de la Administración de la Comunidad Autónoma de las Islas Baleares.

No tan sólo el Ayuntamiento de Palma de Mallorca remite documentos para su publicación al Servicio del BOCAIB, sino que hay más Administraciones públicas implicadas, como son la Administración Periférica del Estado en Baleares, la propia Administración Autonómica, el resto de administraciones municipales, los Consells Insulares, la Administración de Justicia e incluso los particulares. No obstante, en un primer paso, el proyecto se circunscribe a la comunicación telemática entre el Ayuntamiento de Palma de Mallorca y el Servicio de publicación del Boletín Oficial de la Administración de la Comunidad Autónoma, con la intención de extender posteriormente los resultados al resto de administraciones públicas implicadas.

El objetivo del proyecto dentro del cual se sitúa este estudio preliminar consiste así en establecer un nuevo sistema de envío de documentos jurídico-administrativos creados por Ayuntamiento de Palma de Mallorca al Servicio de publicación del BOCAIB dependiente de la Administración autonómica, es decir, pasar del hasta hoy utilizado soporte papel al basado en soporte informático y telemático. De implantarse este sistema de comunicación por vía telemática, podrá conseguirse una reducción de los costes, podrá evitarse cualquier problema de transcripción del contenido de los documentos transmitidos y los tiempos de transmisión podrán igualmente ser reducidos, por lo que se obtendrá un funcionamiento más eficaz en el importante servicio de publicación de documentos en el Boletín Oficial de la Comunidad Autónoma de las Islas Baleares.

Ahora bien, a pesar de las ventajas que la implantación de los medios telemáticos pueden tener en el funcionamiento de este servicio entre las dos Administraciones públicas inicialmente implicadas, no puede olvidarse en *ningún momento que este nuevo sistema de transmisión de documentos ha de contar con el suficiente respaldo* normativo que garantice el mismo grado de validez que el actualmente existente en el envío de documentos en el soporte tradicional de papel. Ha de tenerse muy presente que la publicación de actos administrativos y disposiciones reglamentarias constituye un trámite de gran importancia y trascendencia jurídica.

Así, por ejemplo, de la publicación en el correspondiente Boletín oficial depende que las disposiciones reglamentarias entren en vigor (artículo 2 del Código Civil y 52 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LPAC)) y en determinados supuestos la publicación del acto administrativo es presupuesto para que pueda producir efectos jurídicos (artículo 59.4 LPAC). De esta manera, es fundamental determinar los requisitos jurídicos necesarios cuyo cumplimiento ha de garantizar la validez jurídica de las transmisiones de documentos que se realicen a través de estos medios y sistemas de comunicación telemáticos entre estas dos Administraciones Públicas.

Para la determinación de los requisitos que el sistema de comunicación telemática ha de integrar, conviene en primer lugar determinar secuencialmente las actuaciones que las Administraciones públicas implicadas llevan a cabo en todo el proceso. Estas actuaciones serían las siguientes:

1.- Creación por el Ayuntamiento de Palma del documento en soporte informático que ha de ser publicado en el BOCAIB.

2.- Emisión por vía telemática del documento creado en soporte informático por el Ayuntamiento de Palma al Servicio de publicación del BOCAIB dependiente de la Administración de la CAIB.

3.- Recepción por vía telemática el Servicio de publicación del BOCAIB del documento emitido por el Ayuntamiento de Palma de Mallorca.

4.- Publicación del documento recibido en soporte informático por el Servicio de publicación del BOCAIB en el Boletín Oficial de la Comunidad Autónoma de las Islas Baleares.

Este conjunto de actuaciones pueden agruparse en tres momentos o fases fundamentales, que son:

1ª.- La creación de un documento en soporte informático por el Ayuntamiento de Palma de Mallorca para su posterior transmisión por vía telemática.

2ª.- La transmisión por vía telemática del documento informático creado por el Ayuntamiento de Palma de Mallorca con destino al Servicio de publicación del BOCAIB dependiente de la Administración de la Comunidad Autónoma de las Islas Baleares.

3ª.- Publicación del documento informático recibido por el Servicio de publicación del BOCAIB en el Boletín Oficial de la Comunidad Autónoma de las Islas Baleares.

Mediante el presente estudio debe procederse al análisis de cada una de las fases que acaban de enunciarse desde una doble perspectiva:

- En primer lugar, determinar si de acuerdo con la normativa actualmente en vigor en nuestra Comunidad Autónoma existe base legal suficiente para que cada una de las fases apuntadas pueda ser desarrollada por la administración implicada.

- En segundo lugar, determinar en una primera aproximación los requisitos mínimos que el sistema de comunicación telemática entre ambas Administraciones ha de contener, con la indicación de si éstas cuentan ya en la actualidad con el suficiente respaldo normativo, y en su caso, determinar igualmente qué actuaciones normativas son precisas para que su implantación sea jurídicamente viable.

II.- LA CREACION DE DOCUMENTOS EN SOPORTE INFORMATICO POR EL AYUNTAMIENTO DE PALMA DE MALLORCA:

El primer punto que debe ser objeto de análisis en este estudio consiste en determinar si el Ayuntamiento de Palma puede crear documentos jurídicos en soporte informático. Es éste un presupuesto esencial para la viabilidad del proyecto planteado, por cuanto si el Ayuntamiento de Palma no puede crear un documento en soporte informático con igual validez jurídica que el creado en soporte sobre papel, es obvio que no tiene ya sentido seguir hablando sobre su posible transmisión por vía telemática.

1.- El concepto de documento administrativo y su relación con el acto administrativo:

No obstante, antes de entrar en el análisis de si es viable jurídicamente la creación de un documento administrativo en soporte informático, conviene aclarar previamente qué debe entenderse por documento administrativo. Al respecto, el artículo 46.4 la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LPAC) señala lo siguiente:

"4. Tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones públicas."

En consecuencia, por documento administrativo entenderemos aquel documento que haya sido válidamente emitido por el órgano competente de la Administración pública actuante.

Por otra parte, conviene hacer mención expresa a la diferenciación entre documento administrativo y acto administrativo, en la medida que son conceptos totalmente distintos. Un acto administrativo consiste básicamente en una *declaración de voluntad, de juicio, de conocimiento o de deseo realizada por la Administración pública, mientras que* el documento administrativo constituye la realidad material en que esa declaración de la Administración es plasmada.

Ahora bien, a pesar de tratarse de conceptos claramente diferenciados, lo cierto es que al mismo tiempo se encuentran íntimamente relacionados, en la medida que el documento en el que se plasma el acto administrativo o disposición reglamentaria contiene al mismo tiempo elementos fundamentales determinantes de la validez del acto administrativo mismo o de la disposición reglamentaria. Por tanto, a la hora de determinar la viabilidad de la creación de documentos administrativos en soporte informático, no puede desconocerse que al mismo tiempo se está afectando de una forma más o menos directa a requisitos determinantes de la validez del acto administrativo o *disposición reglamentaria que el documento contiene, por lo que dicho análisis de la viabilidad jurídica de crear* un documento administrativo en soporte informático deberá extenderse, cuando ello sea necesario, al examen del cumplimiento de determinados requisitos determinantes de la validez del acto administrativo.

2.- Los supuestos de creación de documentos administrativos en soporte informático:

Determinados estos conceptos elementales, la cuestión planteada reside, pues, en si el Ayuntamiento de Palma de Mallorca puede crear un documento en soporte informático que contenga un acto administrativo que deba ser objeto de publicación en el BOCAIB. Pues bien, para dar respuesta a esta primera cuestión debe realizarse una *distinción básica relativa a la forma de producción del acto administrativo que contiene el documento informático:*

- En primer lugar, puede tratarse de un acto administrativo que haya sido creado en el seno de un procedimiento tramitado en soporte de papel y que por tanto el acto administrativo haya sido plasmado sobre este soporte tradicional. En este supuesto será preciso crear una copia del documento en soporte informático para su posterior transmisión por vía telemática.
- En segundo lugar, el acto administrativo puede haber sido creado originariamente ya en soporte informático como consecuencia de la tramitación de la totalidad del procedimiento administrativo en ese mismo soporte. En tal supuesto, ya se tiene el documento informático desde el momento de la producción misma del acto administrativo.

La distinción que acaba de realizarse es fundamental por cuanto ambos supuestos hacen referencia a realidades radicalmente diferentes. Así, en el primer supuesto nos encontramos simplemente ante la creación de una copia de un acto administrativo ya existente, mientras que en el segundo supuesto toda la problemática se centra y desarrolla en la creación misma del acto administrativo, el cual nace ya en el seno de un procedimiento informatizado y por tanto se encuentra en este mismo soporte desde el momento de su creación. En este sentido, debe tenerse muy en cuenta que el acto administrativo como declaración realizada por la Administración pública se enmarca necesariamente dentro de un procedimiento administrativo, cuya tramitación da precisamente como resultado la creación del acto administrativo en cuestión. Así resulta de lo establecido en la propia Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que en su artículo 53.1 establece:

"1. Los actos administrativos que dicten las Administraciones Públicas, bien de oficio o a instancia del interesado, se producirán por el órgano competente, ajustándose al procedimiento establecido."

Ello supone, por tanto, que en la creación de documentos administrativos ha de tenerse muy en cuenta su íntima vinculación con el expediente de que trae causa y del que por tanto forma parte integrante.

A.- La creación de copias en soporte informático de actos administrativos creados en soporte sobre papel:

A1.- La viabilidad jurídica de crear copias en soporte informático de actos administrativos creados en soporte sobre papel:

El primer supuesto que acaba de indicarse consiste en que el acto administrativo ha sido creado en el seno de un procedimiento administrativo tramitado en soporte tradicional sobre papel, y una vez que el acto administrativo ya existe sobre soporte papel, se pretende realizar su transmisión por medios telemáticos. En este supuesto, para que sea posible la transmisión telemática, será precisa la previa creación de un documento en soporte informático con el mismo contenido que el documento en que se ha plasmado el acto administrativo en el soporte tradicional de papel, o en otras palabras, deberá crearse un documento administrativo en soporte informático del documento administrativo ya existente en soporte papel.

La cuestión a resolver en este supuesto consiste en determinar la viabilidad jurídica de crear un documento jurídico administrativo en soporte informático que sea copia de uno ya existente en soporte sobre papel, es decir, si es jurídicamente posible crear un documento administrativo en soporte informático de uno ya creado previamente en soporte papel que tenga la misma validez jurídica que el original. Para resolver este primer interrogante debe partirse de lo establecido en el artículo 45.5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LPAC). Este importante artículo se expresa en los siguientes términos:

"Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción pcr el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta y otras Leyes."

La simple lectura de este artículo permite afirmar la plena validez jurídica de un documento administrativo creado en soporte informático, siempre que se garantice su autenticidad, su integridad y su conservación. De este artículo se infiere, pues, que las Administraciones públicas pueden crear documentos administrativos en soporte informático, siempre que quede garantizada su autenticidad, integridad y conservación. Posteriormente se hará referencia a las exigencias que del cumplimiento de estos tres requisitos se derivan.

Ahora bien, el artículo 45.5 LPAC permite afirmar la validez de un documento administrativo creado en soporte informático, pero ha de tenerse en cuenta que en el presente supuesto estamos hablando no tan sólo de la producción de un documento administrativo en soporte informático, sino que además éste debe ser una copia de un documento previamente creado en soporte papel. Por tanto, lo establecido en el artículo 45.5 LPAC debe complementarse con el artículo 46 LPAC que trata de las copias de documentos realizadas por las Administraciones Públicas. Ya se ha señalado anteriormente que el artículo 46.4 LPAC considera como documentos públicos administrativos a los documentos válidamente emitidos por los órganos de las Administraciones Públicas. Pues bien, este mismo artículo, en su apartado segundo, establece lo siguiente:

"Las copias de cualquiera documentos públicos gozarán de la misma validez y eficacia que estos siempre que exista constancia de que sean auténticos."

De la conjunción del artículo 45.5 LPAC relativo a la validez de los documentos administrativos creados en soporte informático y del artículo 46.2 LPAC relativo a la validez de las copias de los documentos públicos (como se ha visto, el artículo 46.4 LPAC considera el documento por los órganos de las Administraciones públicas como documentos públicos) se deduce la plena validez jurídica de un documento administrativo creado en soporte informático como copia de un documento administrativo creado originariamente en soporte de papel, siempre que en la copia exista constancia de su autenticidad.

Por otra parte, y de acuerdo con lo establecido en el artículo 45.4 LPAC, deberá procederse a la previa apro-

bación del programa informático que haya de utilizarse para la creación de las copias informáticas así como para su validación. Concretamente el artículo 45.5 LPAC dispone:

"4. Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características."

A2.- Requisitos de las copias creadas en soporte informático:

a.- De carácter subjetivo: Tal como ya se deriva del artículo 46.4 LPAC, para que un documento administrativo sea válido, ha de ser emitido por el órgano competente de la Administración pública correspondiente. Este artículo debe complementarse con el artículo 46.1 LPAC, que establece:

"Cada Administración Pública determinará reglamentariamente los órganos que tengan atribuidas las competencias de expedición de copias auténticas de documentos públicos o privados." Por tanto, corresponderá al Ayuntamiento de Palma determinar qué órganos del municipio son los competentes para la expedición de copias en soporte informático de documentos administrativos. No obstante, debe tenerse en cuenta también el artículo 204 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Corporaciones Locales, aprobado por Real Decreto 2568/1986, de 28 de noviembre, que en su artículo 204 establece lo siguiente:

"Las certificaciones de todos los actos, resoluciones y acuerdos de los órganos de gobierno de la entidad, así como las copias y certificados de los libros y documentos que en las distintas dependencias existan, se expedirán siempre por el Secretario, salvo precepto expreso que disponga otra cosa."

De este artículo se deriva, por tanto, que en principio es competencia del Secretario de la Corporación municipal la expedición de copias de los documentos administrativos, y por tanto, también, de las copias que deban ser creadas en soporte informático, salvo que exista una disposición que atribuya expresamente esta competencia a otro órgano distinto.

b.- De carácter objetivo:

i.- La autenticidad: Este requisito supone que el documento en soporte informático debe ser atribuible sin ningún género de dudas al órgano de la Administración que efectivamente lo ha creado. En el caso de las copias de documentos originales, este requisito se cumplirá con la garantía de las firmas de los órganos competentes para la emisión de las copias, de acuerdo con lo indicado en el punto anterior.

ii.- La integridad: En segundo lugar, debe garantizarse que la copia creada en soporte informático no va a poder ser alterada en su contenido, ya sea mediante la supresión, adición o modificación de cualquiera de los términos que contiene el documento, ya sea por el propio órgano que en su momento creó el documento o por cualquier otro tercero.

iii.- La conservación: Finalmente, deberá garantizarse por la Administración local un sistema informático de conservación de las copias informáticas por ella creadas, que integre, además, las garantías anteriormente citadas de autenticidad e integradad de los documentos informáticos.

B.- La creación de actos administrativos en soporte informático:

En el apartado anterior se ha examinado la viabilidad jurídica de crear copias informáticas de documentos administrativos creados originariamente en soporte de papel, requisito indispensable para proceder a su posterior transmisión por vía telemática. Ahora bien, cabe por otro lado que la Administración actuante decida la informatización de un determinado procedimiento administrativo, de tal manera que todas las actuaciones integrantes del

mismo se llevarían a cabo en soporte informático. No nos referimos aquí al supuesto en que un determinado documento es creado por medios informáticos y posteriormente imprimido en soporte papel para pasar a formar del expediente administrativo tramitado en soporte papel, sino al supuesto en que el documento es creado en soporte informático e integrado en un expediente administrativo constituido en ese mismo soporte informático, de tal manera que en principio no existe un expediente en soporte sobre papel.

B1.- El programa informático de tramitación del procedimiento administrativo como instrumento integrador del mismo:

La tramitación de un determinado expediente administrativo en soporte informático presupone la existencia de un programa informático que gestione la tramitación misma del procedimiento administrativo, es decir, que la tramitación del procedimiento administrativo se desarrollará sobre la base de un programa informático que en cada momento determinará las actuaciones que han de llevarse a cabo e integrará asimismo el conjunto de actuaciones que hasta un concreto momento se hayan realizado. El programa informático constituye así la base sobre la cual se producirá la tramitación y resolución del procedimiento administrativo. El programa informático es el que determinará en cada momento la fase en que se halla el procedimiento, quién puede actuar y en qué sentido puede llevarse a cabo la actuación. Por tanto, el programa informático se convierte en el instrumento fundamental de establecimiento de las garantías de seguridad y protección, en la medida en que el programa deberá integrar el conjunto de medidas y requisitos pertinentes para garantizar el cumplimiento de los requisitos legalmente establecidos para la existencia de un procedimiento administrativo informatizado.

La Ley 30/1992, consciente de la importancia que tienen el programa informático que ha de servir de soporte al procedimiento administrativo y por tanto del ejercicio de las competencias vinculadas a este procedimiento, le dedica el punto cuarto del artículo 45, anteriormente reproducido. De este artículo conviene destacar ahora la prescripción relativa a la necesidad de aprobación formal del programa por el órgano competente, el cual en el acto de aprobación habrá de determinar el alcance y las condiciones en que el programa ha de ser utilizado.

B2.- La viabilidad jurídica de la tramitación de un procedimiento administrativo en soporte informático:

La primera cuestión que debe tratarse consiste en determinar si es posible la tramitación de un procedimiento administrativo en soporte informático. Esta posibilidad se deriva de lo establecido en el artículo 45.3 LPAC, el cual establece lo siguente:

"3. Los procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y el ejercicio de la competencia por el órgano que la ejerce."

Este artículo contiene tanto el reconocimiento explícito de la admisión de procedimientos tramitados en soporte informático, como la admisión del final del procedimiento administrativo en soporte informático, o en otras palabras, la admisión de la validez de la resolución administrativa, como acto que pone fin al procedimiento administrativo, contenida en soporte informático. No es ya tan solo que la tramitación del procedimiento administrativo, y por tanto de los actos trámite que la integren, se pueda desarrollar en soporte informático, sino que la resolución administrativa, el acto que expresa la decisión final de la Administración en el procedimiento correspondiente, es válida o posible en un soporte magnético, como resultado de la tramitación del correspondiente procedimiento en este soporte. Por otra parte, la admisibilidad de la validez jurídica de un acto administrativo creado en soporte informático aparece ratificada en el artículo 45.5 LPAC, anteriormente analizado al tratar la viabilidad de las copias informáticas de documentos administrativos.

B3.- Requisitos del programa de tramitación del procedimiento administrativo informatizado:

a- Requisitos subjetivos:

Son aquellos destinados a garantizar que en todo momento el acto administrativo, ya sea un acto trámite o acto definitivo, sea creado por el órgano competente. La Ley 30/1992 contempla expresamente este requisito en el

anteriormente reproducido artículo 45.3, estableciendo de esta forma que el procedimiento tramitado y resuelto en soporte informático ha de garantizar la identificación y el ejercicio de la competencia por el órgano que la ejerce.

Ahora bien, en la garantía de este requisito se ha de tener en cuenta que en la tramitación de un mismo procedimiento administrativo pueden intervenir diversos órganos que actúen en función de competencias diferentes en las sucesivas fases de éste. De esta manera, el programa informático habrá de garantizar este requisito en cada una de las sucesivas actuaciones administrativas integrantes del procedimiento administrativo.

Una mención específica debe hacerse a la problemática que plantean los órganos colegiados. En ellos es inherente la existencia de diversos miembros que de forma colegiada participen en las discusiones y toma de decisiones de los asuntos tratados, el resultado de los cuales se recogen en la correspondiente acta en los términos fijados en el artículo 27 LPAC. En estas situaciones parece obvio que el miembro que deberá estar autorizado por el programa informático para la creación y redacción del acta en soporte informático, es áquel a quien la Ley atribuye estas funcions de acuerdo con el sistema tradicional, que es el Secretario del órgano colegiado, el cual tiene asignadas entre otras las funciones de redactar y autorizar las actas de las sesiones (art. 25.3.d) LPAC). Por tanto, ha de entenderse que será el secretario del órgano colegiado quien tendrá que constar habilitado por el programa informático para poder actuar en el momento procedimental oportuno en la creación del documento acreditativo de la decisión tomada por el órgano colegiado.

b.- *Requisitos procedimentales:*

Con este requisito se pretende garantizar el carácter sucesivo en el que deben producirse los actos de tramitación del procedimiento y que acaben con la resolución administrativa. Se trata en definitiva de garantizar que no se podrá dictar un determinado acto, ya sea de trámite o la misma resolución definitiva, sin que previamente hayan sido dictados aquellos actos previos, necesarios para llegar al acto en cuestión.

Este requisito se halla recogido con carácter general en el artículo 75.1 LPAC cuando establece que se acordarán en un solo acto todos los trámites que, por su naturaleza, admitan una impulsión simultanea y no sea obligado el cumplimiento sucesivo. Por tanto, si es obligatorio el carácter sucesivo, el programa informático de tramitación habrá de garantizar que un determinado acto no pueda ser realizado si previamente no se han llevado a cabo los actos que le preceden.

c.- Requisitos objetivos:

Con esta denominación se quiere hacer referencia a los mecanismos de seguridad que el programa informático de soporte del procedimiento administrativo debe contener en relación a la protección de los documentos administrativos que integren el expediente informático. Es una afirmación obvia que el programa informático que sea utilizado en la tramitación de un procedimiento administrativo debe contener los suficientes elementos de protección porque los documentos que integran el expediente no puedan ser modificados o alterado una vez hayan sido creados. Conseguir este objetivo parece un requisito esencial para la viabilidad de la tramitación de un procedimiento administrativo en soporte informático.

La Ley 30/1992 ha recogido expresamente esta exigencia de seguridad en la integridad de los documentos administrativos creados y almacenados en soporte informático al ya reproducido artículo 45.5, el cual vincula la validez de un documento administrativo de estas características a la garantía de su autenticidad, integridad y conservación. Por tanto, tres son los requisitos de validez exigidos por el artículo 45.5 LPAC, los cuales han de analizarse de forma separada:

i.- El requisito de la autenticidad:

La garantía de autenticidad ha de identificarse con la idea de que todo documento administrativo integrante de un procedimiento administrativo que se encuentre almacenado en soporte informático, sea en todo momento el documento creado por el órgano administrativo competente, en el momento procedimental correspondiente. Es

esta una exigencia elemental, de la cual ha de señalarse que se refiere tanto a la protección ante una posible actuación de terceros, como del propio órgano competente que ha dictado el acto. El programa informático debe garantizar que una vez creado un determinado documento en soporte informático por el órgano competente en el momento procedimental adecuado, ya sea constitutivo de un acto trámite o un acto definitivo, éste sea insustituible, tanto por el órgano que lo ha creado, como por cualquier tercero.

ii.- El requisito de la integridad:

En segundo lugar, el programa informático de tramitación del procedimiento administrativo debe garantizar la integridad del documento informático, es decir, no debe posibilitar que por algún lado pueda ser modificado con posterioridad a su creación por el órgano competente. El alcance de este requisito no se refiere tan solo a la sustitución de algunos términos del documento original por unos otros, sino también a la adición de nuevos términos inicialmente no comprendidos en el documento, como la eliminación de otros que si se hallan incorporados en el documento original. Por otro lado, la integridad del documento debe ser protegida tanto de posibles actuaciones del propio órgano actuante como de terceros.

iii.- El requisito de la conservación:

Finalmente, para que un documento administrativo generado y almacenado en soporte informático sea válido, el programa informático de tramitación del procedimiento administrativo debe garantizar su conservación, es decir, debe impedir que el documento pueda desaparecer o ser eliminado del soporte en el que se encuentre almacenado.

No obstante, hemos de ser conscientes que el cumplimiento de este requisito no afecta tan sólo al programa informático de tramitación, sino que se enmarca dentro de una estrategia más amplia que la Administración deberá definir, consistente en la determinación de los medios de almacenamiento de la información en soporte informático, en la medida que existen diversos sistemas de almacenamiento de la información en soporte informático. El programa informático de tramitación deberá garantizar la conservación de los documentos administrativos integrantes del procedimiento a medida que éstos son creados durante la tramitación del procedimiento, pero ha de tenerse presente que el requisito de la conservación se extiende al posterior almacenamiento de la información contenida en el expediente una vez que el procedimiento haya sido terminado y se ordene el archivo de las actuaciones .

III.- LA TRANSMISION POR VIA TELEMATICA DEL DOCUMENTO INFORMATICO CREADO POR EL AYUNTAMIENTO DE PALMA DE MALLORCA CON DESTINO AL SERVICIO DE PUBLICACION DEL BOCAIB DEPENDIENTE DE LA ADMINISTRACION DE LA COMUNIDAD AUTONOMA DE LAS ISLAS BALEARES:

1.- La viabilidad jurídica en la utilización de las técnicas de comunicación telemática entre el Ayuntamiento de Palma de Mallorca y el Servicio de Publicación del BOCAIB:

A.- La viabilidad jurídica en la utilización de las técnicas de comunicación telemática entre Administraciones públicas en general:

Establecido en qué términos el Ayuntamiento de Palma de Mallorca puede crear documentos en soporte administrativo, el siguiente paso que debe darse en la determinación de la viabilidad del proyecto planteado, reside en analizar la viabilidad de la emisión por el Ayuntamiento de Palma de Mallorca de un documento informático por vía telemática dirigido a otra Administración pública como es la Administración de la Comunidad Autónoma. Ello supone, no obstante, plantearse previamente y con carácter general, si es posible la utilización de las técnicas de comunicación telemática en las Administraciones públicas, y la respuesta a esta pregunta ha de ser forzosamente afirmativa por las siguientes razones:

a.- En primer lugar, porque el artículo 45.1 LPAC incluye entre las técnicas y medios que han de ser objeto de impulso por las Administraciones públicas en el desarrollo de sus actividades y el ejercicio de sus com-

petencias, los de naturaleza telemática. Por tanto, existe un mandato legal que con carácter general impone la introducción de esta técnica o medio de comunicación en las Administraciones públicas

b.- En segundo lugar, porque el artículo 45.2 LPAC autoriza expresamente la utilización de medios telemáticos en la comunicación de particulares con la Administración pública en los siguiente términos:

"2. Cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos con respeto de las garantías y requisitos previstos en cada procedimiento."

Esta autorización contenida en el citado artículo 45.2 LPAC no deja ninguna duda sobre la viabilidad jurídica de la comunicación por vía telemática, al menos, entre los particulares y las Administraciones públicas.

c.- El 38.4 in fine LPAC contempla en relación con los registros generales de las Administraciones públicas el establecimiento de sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática y la transmisión telemática de los asientos. Concretamente, el citado artículo lo regula en los siguientes términos:

"Mediante convenios de colaboración suscritos entre las Administraciones Públicas, se establecerán sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática y la transmisión telemática de los asientos."

Este artículo supone la admisión explícita de la utilización de técnicas de comunicación telemática entre Administraciones, aunque se refiere únicamente a la transmisión de datos pertenecientes a los registros generales de entrada de documentos.

d.- En cuarto lugar, porque el artículo 45.5 LPAC reconoce la plena validez de los documentos emitidos por la Administración en soporte telemático, siempre que quede garantizada su autenticidad, integridad y conservación. Por tanto, la admisión de los documentos emitidos mediante medios telemáticos, presupone el reconocimiento explícito de la posibilidad de utilizar estas técnicas de transmisión por la Administración.

No queda, por tanto, ninguna duda sobre la viabilidad jurídica de la utilización de los medios telemáticos en la actividad de las Administraciones públicas, tanto por la declaración genérica contemplada en el artículo 45.1 LPAC, como por las previsiones concretas de los artículos 45.2, 38.4 i 45.5 LPAC.

A diferencia del supuesto de comunicación entre la Administración y un particular, expresamente contemplado por el artículo 45.2 LPAC, no existe en esta ley un artículo que con carácter general autorice de forma expresa este tipo de comunicación entre administraciones públicas. La única referencia que se hace a la comunicación telemática entre Administraciones públicas es el artículo 38.4 in fine, que se ha transcrito anteriormente, y que hace referencia tan solo a la utilización de esta técnica a efectos de transmisión de datos en poder de los registros generales de entrada de documentos de las distintas Administraciones.

No obstante, no existe inconveniente en admitir la comunicación telemática entre Administraciones públicas. Efectivamente, lo primero que ha de señalarse al respeto, es que la declaración genérica del artículo 45.1 LPAC se deriva, una autorización genérica implícita hacia las Administraciones públicas en la instalación y utilización de estas nuevas técnicas. En consecuencia, salvo que una norma prohiba la utilización de estas técnicas en un ámbito concreto de la actuación administrativa, no se ve inconveniente alguno en que la Administración pueda utilizar los sistemas telemáticos como medio de comunicación con otra Administración.

Por otro lado, ha de tenerse en cuenta que la utilización de la comunicación por vía telemática se halla expresamente contemplada por la Ley al menos por un tipo de actuación administrativa, como es el registro de entrada de documentos, materia en la cual, como se ha visto, se establece la necesidad de crear convenios de colaboración para establecer sistemas de intercomunicación y coordinación en este campo, de acuerdo con lo que dispone el artículo 38.4 in fine LPAC.

Otro argumento a favor de la aceptación de la comunicación por vía telemática entre Administraciones públicas reside en la admisión del artículo 45.5 LPAC de los documentos emitidos por medios telemáticos siempre que se cumplan los requisitos de autenticidad, integridad y conservación. En este sentido, ha de señalarse que la ley no establece ningún tipo de limitación subjetiva en la emisión de documentos a traves de estos medios, razón por la que ha de entenderse que la transmisión de documentos por vía telemática puede ir dirigida a cualquier otro operador jurídico, sea un particular u otra Administración pública.

B.- La viabilidad de la comunicación telemática entre el Ayuntamiento de Palma de Mallorca y el Servicio de Publicación del BOCAIB en concreto:

Determinado con carácter general la viabilidad de la comunicación telemática entre Administraciones públicas, debe tratarse a continuación si la comunicación telemática entre la Administración municipal de Palma de Mallorca y la Administración autonómica a través de su Servicio de Publicación del BOCAIB, es posible.

La respuesta a esta cuestión ha de ser de entrada negativa de acuerdo con la normativa actualmente existente del servicio de publicación del BOCAIB. Concretamente, el Decreto 101/1986, de 29 de noviembre, por el cual se establece el Reglamento del Boletín Oficial de la Comunidad Autónoma de las Islas Baleares, se manifiesta en los siguientes términos a la hora de regular la forma de remisión de los documentos que han de ser remitidos a dicho servicio:

"Los originales destinados a la publicación en el BOCAIB deben remitirse mecanografiados o impresos por cualquier procedimiento químico o mecánico, sin tachaduras ni raspaduras."

Este artículo circunscribe, por tanto, las formas de presentación de los documentos a los mecanografiados o impresos por cualquier procedimiento químico o mecánico. Ello supone la exclusión a contrario de los procedimientos informáticos y telemáticos como vía de remisión de los documentos que han de ser publicados en el Boletín Oficial de la Comunidad Autónoma de las Islas Baleares.

La consecuencia de todo ello es evidente, y consiste en que será precisa en todo caso una modificación de esta normativa para habilitar al Servicio del BOCAIB para la recepción de documentos telemático para su publicación en este boletín oficial.

2.- La creación de registros telemáticos de entrada y salida de documentos informáticos:

De acuerdo con lo establecido en la LPAC, las Administraciones públicas han de contar con un registro general de documentos que le permita mantener un estricto control tanto de los documentos recibidos como de los enviados por ellas a terceros. De ello se deduce que la implantación de un sistema de comunicación telemática entre Administraciones públicas, deberá prever un sistema de control específico de los documentos emitidos y recibidos por este medio.

Las características concretas de este registro de documentos telemáticos deberá enmarcarse dentro de la regulación genérica del registro general de documentos, efectuada en un primer nivel por la propia LPAC, la cual en su artículo 38.1 LPAC establece:

"1. Los órganos administrativos llevarán un registro general en el que se hará el correspondiente asiento de todo

escrito o comunicación que sea presentado o que se reciba en cualquier unidad administrativa propia. También anotarán en el mismo, la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares."

Junto con este registro general, la Ley admite la existencia de registros auxiliares, tal como expresa el artículo 38.2 LPAC en su primer parágrafo:

"2. Los órganos administrativos podrán crear en las unidades administrativas correspondientes de su propia organización otros registros con el fin de facilitar la presentación de escritos y comunicaciones. Dichos registros serán auxiliares del registro general, al que comunicarán toda anotación que efectúen."

Conviene tener en cuenta que el propio artículo 38 LPAC en el punto número 3 establece en el primer parágrafo el deber de instalar el registro en soporte informático. Concretamente, el artículo 38.3 LPAC se manifiesta en estos términos en el primer parágrafo:

"3. Los registros generales así como todos los registros que las Administraciones Públicas establezcan para la recepción de escritos y comunicaciones de los particulares o de órganos administrativos, deberán instalarse en soporte informático."

A continuación, el artículo 38.3 establece los datos que deben constar en la práctica de un asiento en el registro, que concretamente vienen expresados en estos términos en el segundo parágrafo del citado artículo:

"El sistema garantizará la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha de entrada, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del escrito o comunicación que se registra."

Finalmente, conviene también destacar el parágrafo segundo del artículo 38.2 LPAC, relativo a la forma en que han de anotarse los asientos::

"Los asientos se anotarán respetando el orden temporal de recpeción o salida de los escritos y comunicaciones, e indicarán la fecha del día de la recepción o salida."

Por otra parte, y en relación al registro de salida del Ayuntamiento de Palma de Mallorca, la regulación que acaba de exponerse deberá complementarse con la contenida en el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Corporaciones Locales (ROF), aprobado por Real Decreto 2568/1986, de 28 de noviembre, concretamente del artículo 151 al 162. De estos artículos conviene señalar el artículo 153.2 ROF, que en relación a los asientos que debe contener el registro de salida establece:

"2. Los asientos de salida se referirán a estos conceptos:

a) Número de orden.

b) Fecha del documento.

c) Fecha de salida.

d) Autoridad, Negociado, Sección o dependencia de donde procede.

e) Autoridad, Corporación o particular a quien se dirige.

f) Extracto de su contenido.

g) Referencia, en su caso, al asiento de entrada, y

h) Obversaciones."

De la regulación que acaba de exponerse relativa al registro general de documentos hay que destacar que el artículo 38 LPAC no entra en la regulación de la forma o soporte en que la documentación dirigida a la Administración ha de presentarse, sino que se limita a regular la forma y requisitos en que debe dejarse constancia en el mismo registro de la entrada o salida de la documentación. Así, prescribe el conjunto de datos que han de constar en la anotación de cada entrada (art. 38.3, 2º), el soporte informático en que se han de introducir los datos (art.38.3, 1º), o el orden cronológico en que deben llevarse a cabo los asientos (art. 38.2, 2º). Pero la Ley 30/1992 no entra en la regulación concreta de la forma de admisión por el registro de los documentos transmitidos por vía telemática.

Ante la suma transcendencia de esta cuestión si quiere establecerse un sistema telemático de transmisión de documentos, es evidente que deberá procederse a su concreta determinación por la Administración que pretenda admitir documentos por vía telemática. A nuestro entender este registro de entrada o de salida de documentos transmitidos telemáticamente debería cumplir al menos con los siguientes requisitos:

- en primer lugar, habrá de tratarse de un registro auxiliar de los previstos en el artículo 38.2, 1º LPAC, por la sencilla razón de que la implantación de este sistema de comunicación será al principio sumamente lenta y en todo caso de alcance muy reducido, y en consecuencia no supondrá, al menos en plazo bastante largo, la desaparición de los registros tradicionales.

- en segundo lugar, deberá garantizar la constancia de los extremos contemplados en el artículo 38.3, 2º LPAC, que como ya se ha visto son el número de entrada, epígrafe expresivo de su naturaleza, fecha de entrada, fecha y hora de presentación, identificación del interesado u órgano remitente y persona u órgano al que se envía, y en su caso, referencia al contenido del escrito o comunicación que se registra.

- en tercer lugar, este registro deberá tener la capacidad de almacenamiento de los documentos objeto de transmisión, con las garantías genéricas de autenticidad, integridad y conservación ya conocidas, mientras se realice todo el proceso de transmisión.

- finalmente, deberá contener un sistema de remisión de los documentos recibidos en los órganos administrativos destinatarios, tan pronto como ésta sea posible, para dar cumplimiento al artículo 38.2.3º.

3.- La determinación del sistema de comunicación telemática entre las dos Administraciones públicas actuantes:

En segundo lugar, para que sea posible la comunicación telemática entre dos o más Administraciones públicas, deberá establecerse el sistema de comunicación telemática que vaya a utilizarse. La propia Ley 30/1992, en el citado artículo 38.4 *in fine*, contempla la necesidad de establecer convenios de colaboración entre las Administraciones públicas para conseguir el objetivo de contar con sistemas de comunicación y coordinación de los registros de entrada y salida de documentos, que garanticen su compatibilidad informática y transmisión telemática. No obstante, la Ley prevé de forma expresa la figura del convenio de colaboración tan sólo para este concreto ámbito de actuación administrativa como son los registros de entrada y salida de documentos, sin establecer una regla general aplicable a la globalidad de supuestos de comunicación telemática entre administraciones públicas.

Así las cosas, tan sólo el artículo 45.4 LPAC puede servir como punto de referencia para establecer una regla general en esta cuestión, el cual, como ya se ha visto anteriormente, establece lo siguiente:

"4. Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características."

De acuerdo con lo establecido en este artículo, y en base a la consideración de que es competencia de la Ad-

ministración de la CAIB la publicación de los documentos pertinentes en el Boletín Oficial de la Comunidad Autónoma, lo más lógico es que corresponda a esta Administración pública la determinación del sistema de comunicación telemática que vaya a utilizarse en la recepción de los documentos que deberán ser publicados en el BOCAIB. Así pues, la Administración de la CAIB deberá proceder a la aprobación del sistema informático y telemático apto para la recepción de los documentos, quien a continuación deberá difundir las características del sistema de transmisión telemática para que los demás sujetos implicados puedan remitir los documentos por esta vía.

4.- Requisitos de seguridad del sistema de transmisión telemática:

Existen una serie de requisitos de seguridad fundamentales que todo sistema de comunicación telemática deberá garantizar. Dos de estos requisitos están expresamente contemplados en el artículo 45.5 LPAC y son la autenticidad y la integridad del documento transmitido telemáticamente. El tercer requisito al que se hace referencia es el requisito de la actualidad de los documentos transmitidos por vía telemática. En cambio, no se considera aquí como requisito que deba tenerse en cuenta la confidencialidad, por cuanto nos encontramos ante un supuesto de transmisión telemática que precisamente tiene como finalidad remitir documentos al Servicio de publicaciones del BOCAIB, servicio que tiene como función publicar tales documentos en el BOCAIB para darles publicidad.

Concretamente, el sistema de transmisión telemática deberá garantizar los siguientes requisitos:

a.- Requisito de la autenticidad: La autenticidad consiste en que el documento emitido por el emisor pueda ser atribuido exclusivamente a éste por parte del receptor. A los efectos concretos del presente supuesto de comunicación telemática entre el Ayuntamiento de Palma de Mallorca y el Servicio del BOCAIB, conviene señalar que el artículo 9. g) del Decreto 101/1986, de 20 de noviembre, que aprueba el Reglamento del BOCAIB, establece en relación a la recepción de documentos de otras Administraciones públicas no contempladas anteriormente (y entre las que no se encuentra las Administraciones locales) que corresponde a las Autoridades que tengan atribuida la representación de cada entidad u organismo, la remisión de los documentos que han de ser objeto de publicación el BOCAIB. Ello suppone que de acuerdo con lo establecido en el artículo 21.1b) de la Ley 7/1985, de 2 de abril, de Bases del Régimen Local, corresponderá al Alcalde del Ayuntamiento la remisión de los documentos que deban ser publicados en el BOCAIB.

b.- Requisito de la integridad: Esta garantía ha de permitir evitar que cualquier tercero pueda modificar parte o la totalidad del documento emitido por el emisor, hecho que en este caso se produciría durante la realización de la transmisión telemática.

c.- Requisito de la actualidad: Mediante esta garantía se pretende asegurar la no repetición de documentos ya transmitidos con anterioridad.

5.- La problemática del acuse de recibo:

Queda por tratar, como última cuestión, la problemática del acuse de recibo de la transmisión telemática. Realizada un determinada transmisión de un documento por vía telemática, al emisor debe remitírsele un acuse de recibo que le permita probar la emisión del documento y que éste ha sido efectivamente recibido por el receptor.

El acto de transmisión del acuse de recibo por el receptor al emisor ha de cumplir dos importantísimos requisitos como son:

- en primer lugar, el acuse de recibo ha de efectuarse en un corto plazo de tiempo a la transmisión del documento por el emisor, casi de inmediato tendríamos que decir, para que éste pueda conocer de forma inmediata que efectivamente su mensaje ha sido recibido por la Administración receptora.
- en segundo lugar, el acuse de recibo ha de contener de una forma incorruptible la fecha y la ho-

ra exacta de recepción por la Administración del documento emitido por el emisor, ya que este dato se configura como un elemento fundamental de la validez o temporaneidad de la actuación del emisor.

La cuestión que a continuación ha de plantearse consiste en determinar las consecuencias de la no emisión del acuse de recibo por la Administración receptora del documento, ya sea por problemas técnicos o bien por negligencia o dolo de la Admininistración receptora. La cuestión tiene bastante trascendencia, dada la actual regulación que contiene el Decreto 101/1986, de 20 de noviembre, el cual en su artículo 13 dipone:

"Los anuncios que fijen unos plazos de efectividad deberán remitirse con la antelación suficiente para que los mismos puedan cumplirse. Caso de que sea imposible su publicación dentro de los plazos previstos, se devolverán a sus centros emisores para su rectificación."

Por tanto, puede resultar de suma importancia que el emisor de un documento cuente necesariamente con un acuse de recibo, para determinar si ha cumplido o no dentro del plazo correspondiente el deber de remitir al Servicio del BOCAIB el documento para su publicación.

Ante esta situación, no hay otra solución que introducir la figura de un tercero, que ya sea con carácter principal o subsidiario, que ante el requerimiento del emisor, remita el documento a la Administración, sirviendo al emisor como prueba suficiente de presentación del documento el acuse de recibo del tercero, sin que la Administración receptora pueda negar haber recibido el documento.

Esta solución es, no obstante, muy problemática, por cuanto supone dotar a este tercero de unos poderes altamente vinculantes para la Administración en un punto tan importante como es la recepción de documentos por la Administración y su vinculación con el registro de documentos. Es evidente, por tanto, que deberá existir una normativa que confiera estos poderes a este tercero, o lo que es lo mismo, dotarle de un estatuto de fedatario público que asuma estas funciones frente a la Administración. Por otro lado, la normativa que desarrolle la figura de este tercero, habrá de contemplar expresamente los supuestos en que puede intervenir y los requisitos que habrá de cumplir en su actuación.

El papel que este tercero podría jugar, pero que en todo caso requerirá de la indicada actuación normativa por parte de la Administración autonómica en el momento de regular el sistema de comunicación telemática, reside en la atribución a cada uno de los sujetos implicados de un buzón informático, que gestione ese tercero, de tal manera que los sujetos implicados, como por ejemplo el Ayuntamiento de Palma de Mallorca, deposita en el buzón los documentos dirigidos a la Administración autonómica, constituyendo este acto de deposito, el envío a ésta del documento que ha de ser publicado en el BOCAIB.

En el momento del depósito del documento en el buzón telemático del tercero, éste debería emitir a la Administración pública emisora un acuse de recibo, que vincularía a todos los efectos a la Administración receptora, esto es, a la Administración autonómica. La normativa reguladora de esta figura deberá necesariamente determinar el alcance y requisitos de esta vinculación, así como el régimen de responsabilidad de este tercero por posibles actuaciones negligentes o dolosas en el cumplimiento de sus funciones.

IV.- PUBLICACION DEL DOCUMENTO INFORMATICO RECIBIDO POR EL SERVICIO DE PUBLICACION DEL BOCAIB EN EL BOLETIN OFICIAL DE LA COMUNIDAD AUTONOMA DE LAS ISLAS BALEARES:

En relación a este punto, el mismo no plantea mayores problemas en la medida que se trata de una actividad administrativa puramente material. Lo único que debe significarse consiste en que de acuerdo con el artículo 45.4 LPAC deberá aprobarse formalmente el programa informático que se utilice para la realización de las tareas propias de confección de los boletines oficiales.

V.- CONCLUSIONES:

De acuerdo con lo expuesto hasta este momento, pueden ya determinarse una serie de conclusiones relativas a la viabilidad jurídica del proyecto planteado de remisión de documentos jurídico-administrativos por vía informática creados por el Ayuntamiento de Palma de Mallorca con destino al Servicio de Publicación del BOCAIB dependiente de la Administración de la CAIB. Partiendo de la estructuración efectuada en este estudio basada en tres fases fundamentales, estas conclusiones serían las siguientes:

I.- En relación a la viabilidad jurídica de creación de documentos administrativos en soporte informático por el Ayuntamiento de Palma de Mallorca:

1º.- Es jurídicamente viable la creación de copias en soporte informático de documentos administrativos creados en soporte de papel. Para ello, en principio, no es precisa ninguna modificación normativa, sino que sería suficiente con la aprobación del correspondiente programa informático por el órgano competente de la Administración municipal, siempre que éste cumpla los requisitos señalados en el correspondiente epígrafe de este estudio.

2º.- Es jurídicamente viable la tramitación de procedimientos administrativos en soporte informático y por tanto la creación de actos administrativos directamente en este soporte. En principio, y con carácter general, no se considera necesaria ninguna modificación normativa para su admisibilidad, aunque este punto deberá determinarse en relación a cada procedimiento concreto en virtud de sus específicas características. En todo caso, esta afirmación se circunscribe a procedimientos sin intervención de interesados o terceros en el mismo, por cuanto no se ha tratado en este trabajo la problemática de la incorporación al expediente informático de documentos aportados por los interesados o terceras personas en dicho soporte, por exceder de la finalidad del mismo.

II.- En relación al establecimiento de un sistema de comunicación telemático entre el Ayuntamiento de Palma de Mallorca y el Servicio de Publicaciones dependiente de la Administración de la CAIB:

1º.- Es jurídicamente viable con carácter general el establecimiento de un sistema de comunicación telemática entre ambas Administraciones, de acuerdo con lo establecido en la LPAC.

2º- No obstante, deberá procederse a la modificación del Decreto 101/1986, de 29 de noviembre, por el cual se establece el Reglamento del Boletín Oficial de la Comunidad Autónoma de las Islas Baleares, para que de forma expresa recoja la posibilidad de recibir por vía telemática los documentos remitidos mediante este sistema de comunicación por el Ayuntamiento de Palma de Mallorca.

3º- Además, deberá estructurarse tanto por el Ayuntamiento de Palma de Mallorca como como por la Administración autónoma de los correspondientes registros auxiliares de entrada y salida de documentos telemáticos, así como el sistema informático interno de recepción de los documentos que hayan de ser remitidos por el Registro de salida del Ayuntamiento y de remisión por el Registro de entrada de la Administración Autonómica al Servicio de Publicación.

4º.- Igualmente, deberá procederse por la Comunidad Autónoma de las Islas Baleares a la aprobación de la correspondiente normativa que regule el sistema de transmisión telemática de documentos, el cual deberá garantizar los requisitos determinados en el epígrafe correspondiente de este trabajo.

5º.- Especial trascendencia en la indicada regulación del sistema de transmisión deberá darse a la

figura del acuse de recibo. Deberá tratar expresamente el papel que haya de atribuirse a un posible tercer intermediario en la transmisión telemática, regulando las funciones que pueda llevar a cabo y sobre todo el grado de vinculación de las mismas hacia la Administración autonómica.

III.- En relación a la publicación por el Servicio de Publicaciones de la administración autonómica, deberá procederse a la aprobación del programa informático que se utilice en la confección de los boletines por el órgano competente, el cual deberá garantizar en todo caso la integridad de los documentos informáticos tratados.

El Consejo General del Poder Judicial y la homologación y Compatibilidad de los Sistemas Informáticos en España.

Francisco Monterde Ferrer (España)
Magistrado. Vocal de la Comisión de Informática del CGPJ de España

I.- PRESENTACION

El Consejo General, según el art. 122.2 de la Constitución española de 1978, es el órgano de gobierno del Poder Judicial, que se ejerce –según el art. 117.3 del mismo texto constitucional- por los Juzgados y Tribunales determinados por las leyes, a quienes corresponde juzgar y hacer ejecutar lo juzgado, conforme a las normas de procedimiento que las leyes establezcan.

Y está integrado:

- Por el Presidente del Tribunal Supremo que lo presidirá, y

- Por veinte miembros nombrados por el Rey por un período de cinco años.

De éstos, doce entre Jueces y Magistrados de todas las categorías judiciales, en los términos que establezca la Ley Orgánica; cuatro a propuesta del Congreso de los Diputados y cuatro a propuesta del Senado, elegidos en ambos casos por mayoría de tres quintos de sus miembros, entre Abogados y otros juristas, todos ellos de reconocida competencia y con más de quince años de ejercício en su profesión.

La L.O.P.J. tras su reforma de 1985 precisa en su art. 112.3 que respecto de los Jueces y Magistrados, cada Cámara legislativa propondrá, también por mayoría de 3/5 de sus miembros, seis vocales.

La misma L.O.P.J. en su art. 117 añade que los miembros del Consejo desarrollarán su actividad con dedicación absoluta, siendo su cargo incompatible con cualquier otro puesto, profesión o actividad, públicos o privados. Su situación administrativa para los que sean funcionarios públicos, tanto judiciales como no judiciales, será la de servicios especiales.

Son atribuciones del CGPJ, entre otras:

1) La propuesta por mayoría de 3/5 del Presidente del Tribunal Supremo y del CGPJ.

2) La propuesta por mayoría de 3/5 de miembros del Tribunal Constitucional.

3) La Inspección de los Juzgados y Tribunales.

4) La selección, formación, perfeccionamiento, provisión de destinos, ascensos, situaciones administrativas y régimen disciplinario de Jueces y Magistrados.

5) Nombramiento de Jueces, Magistrados y cargos judiciales de designación.

6) Nombramiento del secretario General del Consejo y miembros de los gabinetes o Servicios dependientes de los mismos .

7) Potestad reglamentaria.

8) Publicación oficial de la Colección de Jurisprudencia del TS.

9) Información de los Anteproyectos de Leyes y Disposiciones del Estado y de las Comunidades Autónomas que afecten a determinadas materias.

10) Ser oído con carácter previo al nombramiento del Fiscal General del Estado.

11) Elevación anual a las Cortes Generales de una Memoria sobre el estado, funcionamiento y actividades del Consejo y de los Juzgados y Tribunales de Justicia, y necesidad de personal, instalaciones y recursos.

El funcionamiento del Consejo se produce en Pleno y en distintas Comisiones legales y reglamentarias.

Su trabajo se desarrolla esencialmente en tres centros:

- Sede principal, en Madrid, Calle Marqués de la Ensenada número 8.
- Escuela Judicial, en Barcelona, carretera de Vallvidriera 43-45. Collserolla (Barcelona).
- Centro de Documentación y Publicaciones (CENDOJ). Calle Manterola 13 (Donostia-San Sebastián)

II.- INTRODUCCION

Recientemente en una reunión del Pleno del Consejo decía un compañero que la Informática debía ser algo así como la *logística del progreso*. Y probablemente debamos mostrarnos de acuerdo con él. No se agotarán con ella todas las aportaciones materiales que habrán de hacerse para la modernización judicial, pero por la Informática pasa necesariamente cualquier intento de mejora de medios y prestaciones.

En el VI Congreso Iberoamericano de Derecho e Informática que tuvo lugar en Montevideo en mayo de 1998 el representante venezolano Dr. Peñaranda Quintero nos decía que la *Informática Jurídica es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora en el derecho; es decir la ayuda que que este uso presta al desarrollo y aplicación del derecho.*

Y en el mismo evento se insistía por la representantes uruguayas Dras. Bello y Dufau en que *todos los Poderes Judiciales enfrentan los problemas que plantea la masificación en la Administración de Justicia debida a la creciente litigiosidad en las relaciones sociales, lo cual ha generado una progresiva congestión de los despachos judiciales, y que ante ello la modernización del Poder Judicial pasa por la necesidad de dar respuestas adecuadas y oportunas a las demandas de los ciudadanos, atendiendo al estado de insatisfacción generalizada respecto a los servicios que reciben.*

Por supuesto que debemos compartir y compartimos tales opiniones.

El propio Consejo General del Poder Judicial español en su Libro Blanco (pags. 114 y 115) de 1997 señala que:

A) La incorporación de los medios informáticos es necesaria e inaplazable.

B) Debe entenderse en su concepción moderna y actual: como ordenación del proceso, ayuda a la decisión, sistema integrado e intercomunicado.

C) Su utilización debe ser imperativamente exigida.

D) Es necesario realizar un esfuerzo serio, coordinado y urgente, que permita dotar a toda la organización judicial de este instrumento.

E) No se puede hablar de reforma de la justicia sin la informatización de los órganos judiciales.
F) Procede el llamamiento a las Administraciones Públicas para que una de las prioridades presupuestarias sea, precisamente, la instalación de esa red informática.

G) No cabe poner en duda que las mejoras de organización de la justicia pasan, casi en el s. XXI, por tener un sistema informático integral.

Por su parte el Pleno del Congreso de los Diputados -una de las dos cámaras del órgano legislativo español-, en sesión de 13 de mayo de 1.999, aprobó, en relación con la Memoria del CGPJ de 1997 una serie de resoluciones y en la primera de ellas se decía: *El Congreso de los Diputados insta al Gobierno a dotar los recursos necesarios, en el ámbito de sus competencias, para que pueda llevarse a cabo la informatización íntegra de la Administración de Justicia, a fín de conseguir un mayor y mejor conocimiento y control sobre la situación real de los Juzgados y Tribunales que permita a los órganos de gobierno de los mismos actuar donde se detecten disfunciones de cualquier orden, y con ello prestar un mejor servicio público de la justicia a los ciudadanos.*

No hace aún mucho tiempo, ante alguna información periodística tuvimos ocasión desde la Comisión de Informática puntualizando aquélla, de precisar que la implantación de un verdadero sistema informático en el ámbito judicial que satisfaga las necesidades de *registro, tramitación, estadística, inspección y comunicaciones,* supone la renuncia al texto libre que no deja huella en el proceso informatizado y la sumisión de todo el personal usuario a una cierta disciplina en la introducción de todos los datos precisos, en el respeto de todos los esquemas de tramitación y en el formato obligatorio de aquella parte que resulte necesaria de las resoluciones que abran o cierren fase procesal.

Salvados estos aspectos imprescindibles, podrá discutirse con los técnicos informáticos, la mayor o menor rigidez del sistema; pero en beneficio de la modernización definitiva de las oficinas judiciales, todos: magistrados, jueces, secretarios y funcionarios habremos de poner de nuestra parte la mejor voluntad, prescindiendo de inercias interesadas o de cómodas actitudes de rechazo global, contribuyendo a la adopción del sistema que pueda proporcionar a la Administración de Justicia la agilidad y eficiencia que corresponde.

III.- NORMATIVA APLICABLE

Después de aprobarse el texto constitucional en 1978, aparece la L.O.P.J. 6/85 de 1 de julio.

Dispone el art. 37 de la L.O.P.J., en su nº 1 que corresponde al Gobierno a través del Ministerio de Justicia, proveer a los Juzgados y Tribunales de los medios precisos para el desarrollo de su función con independencia y eficacia.

Y añade en su nº 3. *Podrá atribuirse a las Comunidades Autónomas la gestión de todo tipo de recursos ,cualquiera que sea su consideración presupuestaria, correspondientes a las competencias atribuidas al Gobierno en el apartado 1 de este artículo, cuando los respectivos Estatutos de Autonomía les faculten en esta materia.*

La sentencia del TC. 56/90 de 29 de marzo (BOE 4-5-90), declaró nulo un párrafo 4º del mismo artículo, y perfiló con claridad lo que debía considerarse en sentido estricto "Poder Judicial", entendiendo transferible la gestión de los medios materiales, personal auxiliar, médicos forenses y otro personal colaborador comprendido para el concepto acuñado de "administración de la Admón de justicia".

La LOPJ establecía en su art. 230 simplemente que *podrán utilizarse en el proceso cualesquiera medios técnicos de documentación y reproducción, siempre que ofrezcan las debidas garantías de autenticidad. La ley regulará los requisitos y forma de su utilización.*

En aquellos momentos el desarrollo informático en materia de la Administración de Justicia estaba limitado a unas experiencias llevadas a cabo por el Gobierno de la Generalitat de Cataluña a través de la Fundación *Lluis de Peguera*, y a la puesta en marcha por parte del Ministerio de Justicia, único en aquél momento con competencias en la materia, del llamado *Proyecto INFORIUS*.

La situación comienza a cambiar sustancialmente en cuanto que el RD 1.648/87, de 6 de noviembre produce el primer traspaso de competencias en materia de Administración de Justicia al Gobierno Autónomo Vasco, siguiendo el RD 966/90 de 20 de julio a la Generalitat Catalana.

A partir de este momento las Comunidades Gallega, Valenciana, Canaria y Andaluza se suman a este proceso que aún no ha concluido (Navarra, Madrid etc).

Tal asunción de competencias produce como primer efecto el que las distintas Comunidades comenzaran a definir sus modelos informáticos, como así lo hicieron los Gobiernos Vasco y Catalán (PRAOJ, THEMIS I y II), que el Ministerio de Justicia, en el ambito territorial de sus once Comunidades no transferidas, hiciera lo propio (Proyectos LIBRA, CORTE y LINDE), como también Andalucía (Proyecto ADRIANO), y que Galicia Canarias, y Valencia acogieran el sistema del Ministerio, si bien estas dos últimas han iniciado recientemente el desarrollo de aplicaciones propias (*proyectos* ATLANTE *y* CICERONE, *respectivamente*).

A la vista de la situación existente y de la que se podía adivinar como próxima, la L.O. 16/94, de 8 de noviembre, que reformó la LOPJ, procedió a dar al artículo 230 una nueva redacción más acorde con las realidades técnicas del momento.

Y así contempló los usos electrónicos, informáticos o telemáticos en el desarrollo de las funciones de los Juzgados y Tribunales, previendo la validez de los documentos emitidos por tales medios, salvaguardando la autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

Igualmente reguló la tramitación informática de los procesos judiciales, poniendo especial énfasis en las garantías de confidencialidad, privacidad y seguridad en los datos contenidos en el sistema.

Contempló la comunicación no sólo entre los distintos órganos judiciales, sino la de los interesados o profesionales con los mismos; poniendo especialmente el acento en la custodia y gestión de los ficheros automatizados, tal como impone la LO 5/92 sobre protección de datos informáticos.

Y finalmente el artículo de referencia en sus dos últimos párrafos estableció que *Los programas y aplicaciones informáticos que se utilicen en la Administración de Justicia, deberán ser previamente aprobados por el CGPJ, quien garantizará su compatibilidad*; y que los sistemas informáticos que se utilicen en la Administración de Justicia deberán ser compatibles entre sí para facilitar su comunicación e integración, en los términos que determine el CGPJ.

IV.- NORMALIZACION Y COMPATIBILIDAD

El citado precepto de la LOPJ fue objeto de desarrollo reglamentario en los arts. 89 y ss. del Reglamento 5/95, de 7 de junio sobre Aspectos Accesorios de las Actuaciones Judiciales.

En este Reglamento se constituyó la Comisión de Informática Judicial, considerada por su Exposición de Motivos como el *instrumento necesario para la actuación del Consejo* en esta materia.

Presidida por un Vocal del Consejo, está integrada por un Magistrado perteneciente a cada una de las ramas jurisdiccionales: Penal, Civil, Contencioso-Administrativa y Social, y asistida por el Letrado-Jefe del Gabinete Técnico, pudiendo recibir los asesoramientos necesarios por parte de los especialistas y técnicos que corresponda en cada momento.

Entre sus competencias cabe señalar que *deberá proponer al Pleno del CGPJ la determinación de los elementos que han de reunir los sistemas informáticos que se utilicen en la Administración de Justicia para cumplir las exigencias de compatibilidad necesaria en cuanto a su comunicación, integración y seguridad.*

La Comisión procedió a elaborar un documento preliminar estableciendo los elementos básicos que habrían de marcar su trayectoria con el objetivo de alcanzar aquellos fines de homologación que le habían sido marcados respecto de los diferentes sistemas que venían implantando el Ministerio de Justicia y las Comunidades Autónomas con transferencias.

Los trabajos preparatorios de la Comisión dieron como resultado la emisión de un informe que, conocido como *Documento de Cáceres* por haber sido aprobado por el Pleno del Consejo celebrado en dicha Ciudad en diciembre de 1996, sentó los parámetros de Compatibilidad de los Sistemas Informáticos.

El texto llegó a definir a tales efectos qué había que entender por *Organos judiciales, usuarios del sistema, intervinientes, asuntos, registro, número de identificación general (NIG.), trámite, esquemas de tramitación, fases procesales, estados de los procedimientos, puntos de control, documentos, control de accesos y comunicaciones internas y externas.*

Con el objetivo de desarrollar el referido Documento, se creó un Grupo de Trabajo, integrado por el CGPJ, el Ministerio de Justicia y las Comunidades Autónomas de Cataluña, el País Vasco y Andalucía con el objetivo de elaborar un test de compatibilidad para determinar si los sistemas informáticos que hayan de someterse a la aprobación del Consejo reúnen los requisitos de compatibilidad que se pretenden.

Sentadas las bases del "test", de su formalización se encargó la empresa que resultó adjudicataria del correspondiente concurso convocado por el Consejo, firmándose el contrato el 9-12-98.

El resultado de los trabajos presentados por la empresa adjudicataria fueron autorizados por la Comisión de Informática en 19-7-98, que elevó al Pleno la propuesta de aprobación que fue aceptada, efectuándose la presentación pública del "test" en Octubre de 1999.

V.- DESCRIPCION TECNICA DEL TEST

Huyendo de complejidades nos referiremos, nada más y muy sintéticamente, al ámbito de aplicación, a sus funcionalidades, componentes y marcos de referencia.

El ámbito de aplicación del "test"se circunscribe a los sistemas informáticos que se utilicen en los órganos judiciales para el desarrollo de la *gestión* procesal, esto es para la actividad de tramitación de los asuntos jurisdiccionales.

Los requisitos mínimos o funcionalidades que han de contener los distintos sistemas son los siguientes:

- Registro de expedientes.
- Gestión de tramitación.
- Editor-compositor de documentos.
- Mecanismos relacionados con el impulso procesal.

Los componentes del test, vienen a ser las especificaciones diseñadas para poder realizar la evaluación de cada sistema. Y se basan en los siguientes conceptos principales:

- Intercambio de información.

  - Capacidad de intercambio de datos con otros sistemas judiciales y con el Centro de Documentación Judicial.

- Seguridad y Auditoría.

  - Capacidad del sistema para asegurar la confidencialidad, autenticidad e integridad de la información.

- Estadísticas.

  - Capacidad de confeccionar las estadísticas requeridas por el CGPJ.

Pero al respecto hay que aclarar que en esta *primera versión* del test se definen los requerimientos relativos a los dos primeros conceptos, quedando las especificaciones relativas a las Estadísticas para su definición en una versión posterior del Test, que a fecha de hoy ya se ha realizado.

Los documentos básicos que definen las especificaciones requeridas y que constituyen la aplicación del Test sobre un sistema informático concreto son dos:

A) Cuestionarios a cumplimentar. Son nueve en total :

1.- Definiciones comunes.

2.- Solicitud de cooperación jurisdiccional.

3.- Devolución de cooperación jurisdiccional.

4.- Envío de recurso interpuesto.

5.- Devolución de recurso.

6.- *Remisión de asunto completo.*

7.- Envió de resoluciones al Centro de Documentación Judicial. (CENDOJ).

8.- Envío de notas de condena al Registro Central de Penados y Rebeldes.

9.- Seguridad y Auditoría.

Cada uno de los cuestionarios se compone de dos tipos de especificaciones que se corresponden con dos grados distintos de cumplimiento de las exigencias de compatibilidad, uno inferior denominado Nivel 1 que contiene el catálogo de los requerimientos más básicos y fundamentales, y otro denominado Nivel 2 que comprende todos los requerimientos que se plantean como exigencia final por el Consejo General del Poder Judicial.

Se confía en que tras un corto periodo transitorio, todos los sistemas informáticos que existen en la actualidad puedan alcanzar, al menos el primer Nivel, adaptándose paulatinamente en un plazo más dilatado a los requerimientos del Nivel 2 o definitivo.

B) Informe de compatibilidad. Es el producto principal que se obtiene de la aplicación del test. Para realizarlo se tendrán que haber cumplimentado previamente los cuestionarios del Test. Este informe ha de mostrar fundamentalmente los aspectos que el sistema de información debe subsanar para

llegar a ser compatible. El informe deberá acompañarse de toda la información justificativa del sistema que avale el cumplimiento de las especificaciones.

El documento incorpora unos marcos de referencia necesarios para establecer un lenguaje inequívoco y correcto para su definición. Son los siguientes:

a) Modelos de datos de referencia. Define los datos y relaciones de la información denominada estática que un sistema de información al servicio de la Admón. de Justicia debe contemplar para ser compatible.

b) Especificación técnica de los esquemas de tramitación. Supone la definición de un lenguaje técnico y único de expresión para los esquemas de tramitación, realizándose de forma homogénea y siguiendo una formalización concreta de manera que los distintos sistemas informáticos puedan asumir y utilizar dichos esquemas en sus programas de tramitación-

c) Registro de acontecimientos procesales. Se refiere a la definición de los datos y relaciones de la denominada parte dinámica. Se trata de la información relativa a la vida procesal o tramitación de un expediente: estados del procedimiento, puntos de control, fases, etc.

Además para la modelización de datos el test incorpora un repositorio de datos con todos los códigos que existen en los distintos sistemas de información. Previéndose, no obstante que tal codificación pueda sufrir variaciones una vez que se incorporen al Test las especificaciones relativas a la Estadística.

No puede olvidarse tampoco para la aceptación y homologación del sistema de gestión procesal de que se trate, un aspecto cual es el de la operatividad, es decir su manejabilidad por el usuario, entorno más o menos amigable en que se desarrolla, y, en definitiva, si sirve en la práctica para el objeto para el que está diseñado.

VI.- ESTADISTICA

Antecedentes. La segunda fase del Test comprende las Estadísticas y los marcos de referencia afectados (codificación).

El trabajo ha sido presentado a la Comisión de Informática del CGPJ en 28-2-2000, y pende aún de su aprobación definitiva.

Objetivo. Su objetivo está constituido por la identificación y definición de las variables estadísticas contenidas en los boletines, orientada y destinada a los constructores de sistemas informáticos a fin de que puedan diseñar los programas necesarios para ofrecer los datos requeridos.

La referencia a los boletines supone que se distinga entre los actuales, en vigor desde el 1-1-99, y revisados el 1-1-2000, y otros futuros para entornos completamente informatizados.

Tratamiento de la información. La estructura distingue entre Boletines, Bloques, Variables y Agrupaciones.

Y dos niveles de cumplimiento:

- Nivel 1: movimiento de asuntos, ejecuciones y exhortos.

- Nivel 2: escritos pendientes de proveer, recursos, resoluciones, control de señalamientos, situación de los intervinientes y cuestiones muy específicas de algunos boletines.

Finalmente, en el desarrollo del componente de estadísticas, necesariamente hay que utilizar valores codificados.

Así por ejemplo, en los juicios posesorios, si se trata de Interdictos de Adquirir se utilizará *IAD;* si se trata de Interdicto de Retener *IRE.* etc.

Concepto. Más que como un requerimiento o exigencia de compatibilidad aparece la Estadística como el resultado o producto resultante de la aplicación del resto de componentes y marcos de referencia del Test.

VII.- CONCLUSIONES

El Consejo General del Poder Judicial considera que con el Test no sólo se establece el instrumento indispensable para que este órgano constitucional pueda cumplir y hacer cumplir el artículo 230 de la LOPJ sino que también se facilita a las distintas Administraciones con competencia en materia de informatización de la Admón. de Justicia el punto de referencia adecuado al objeto de que sus proyectos y actuaciones resulten, en definitiva, homologados mediante la aprobación del CGPJ y garantizada la necesaria compatibilidad.

Las exigencias del Test no son caprichosas, sino que tienen por finalidad el conseguir que la Administración de Justicia se incorpore de manera decidida y firme a los modernos sistemas de trabajo, que se caracterizan por su carácter integral y sistemático.

La informatización no se puede concebir como una mera aportación de medios materiales, sino que lo más importante es la propia concepción y entendimiento de la informatización.

La correcta implantación de aplicaciones informáticas de gestión procesal –respetando siempre las normas vigentes- ha de conseguir armonizar los métodos de trabajo de los órganos judiciales, sin que por ello quede afectada *la independencia judicial.*

Debe destacarse que, precisamente, la *seguridad jurídica* a que se refiere el art. 9.3 de la Constitución se ve favorecida con dicha armonización que ha de contribuir a que los ciudadanos pasen a tener una relación con la Administración de Justicia muy distinta, más ágil, más clara y más uniforme.

Tema 5

DERECHO EMPRESARIAL Y CORPORATIVO E INFORMATICA EN EL NUEVO MILENIO

La influencia de la Internet en el Marco Regulatorio de las Fusiones y Adquisiciones Corporativas, en los Estados Unidos de América y en México.

Juan Antonio Rangel Charles* **(México)**

Abreviaturas

CNBV - Comisión Nacional Bancaria y de Valores
LBO'S - Leveraged buyouts
LGSM - Ley General de Sociedades Mercantiles
LMV - Ley del Mercado de Valores
MBCA - Model Business Corporation Act
RMBCA - Revised Model Business Corporation Act
SEC - Securities and Exchange Comission

1.- INTRODUCCION

El 24 de enero del año 2000, The Wall Street Journal anunció que el grupo mexicano Sanborn's, adquirió CompUSA, corporación estadounidense cuyo negocio es la venta al menudeo de computadoras personales, que opera actualmente 217 tiendas en los Estados Unidos, y emplea alrededor de 20,000 personas.[1]

El 9 de marzo del mismo año, el diario norteamericano hizo pública la fusión celebrada entre el banco español Bilbao Vizcaya Argentaria BBVA y el Grupo Financiero Bancomer de México, de la cual nació BBVA-Bancomer que será la entidad de servicios financieros más grande de México.[2]

A la pregunta ¿qué tienen en común esas dos operaciones, además de que involucran a grupos empresariales mexicanos? puede responderse con seguridad: que ambas se celebraron en el ámbito de un mercado global que ha sentado sus bases gracias a los avances tecnológicos.

Hoy en día quien desee participar en mercados de otros países, buscando capital o colocando una inversión, solamente tiene que introducir la dirección apropiada en su navegador de la internet.

La actividad de inversionistas extranjeros, propicia la convergencia de los mercados regionales en un centro financiero global, que está conduciendo a las legislaciones nacionales a cambiar, tanto en términos de sofisticación, como en expectativas de seguridad para los participantes.

En tanto las leyes de cada país se adaptan al nuevo ambiente, resulta de gran importancia conocer cómo el derecho de países más desarrollados, ha pretendido salvaguardar los niveles de protección de los inversionistas y la integridad de sus mercados domésticos, para encarar los retos de un mercado globalizado.

En nuestro continente, los Estados Unidos de América poseen el marco regulatorio más avanzado de la actividad empresarial. Adicionalmente, como país líder en materia informática, los Estados Unidos han recibido tempranamente los efectos de los cambios tecnológicos, a los cuales no ha podido sustraerse el Derecho Corporativo.

Como vecino y socio comercial de los Estados Unidos, México ha recibido la influencia directa de las instituciones jurídicas norteamericanas, que se manifiesta, entre otras, en las normas antimonopólicas y en las del mercado de valores.

---

*Director del Departamento de Derecho del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Estado de México. (ITESM-CEM) México.

1 Flashes por e-mail. The Wall Street Journal Interactivo. 24 de enero de 2000.
http://interactivo.wsj.com

Partiendo de ese orden fáctico, nuestra ponencia tiene por objeto dar a conocer, en términos generales, los procesos de fusiones y adquisiciones corporativas en los Estados Unidos, sus similitudes y diferencias con las fusiones de sociedades anónimas en México, y la influencia que la Internet ha tenido en el marco regulatorio de tales actividades, en ambos países.

2. EMPRESA, CORPORACION Y SOCIEDAD ANONIMA.

Siguiendo la definición de Mantilla Molina, diremos que la empresa o negociación mercantil, es "el conjunto de cosas y derechos combinados para obtener u ofrecer al público bienes o servicios, sistemáticamente y con un propósito de lucro"[3]

Para alcanzar su finalidad, una empresa puede adoptar diversas formas de organización, que van desde el propietario individual, hasta la creación de entes ficticios sujetos de derechos y obligaciones.

La corporación en el Derecho de los Estados Unidos de América, es una forma de organización empresarial, definida como aquella entidad legal creada estatutariamente, con personalidad propia y distinta de la de sus accionistas, quienes por lo general tienen responsabilidad limitada al monto de sus aportaciones sociales.[4]

la constitución de las corporaciones está regulada por leyes estatales de corporaciones generales, algunas de las cuales han incorporado normas tanto de la Model Business Corporation Act, como de la Revised Model Business Corporation Act.[5]

La MBCA fue un proyecto de ley uniforme de corporaciones, elaborado en 1950 por la American Bar Association, en tanto que la RMBCA, es una revisión de la MBCA que se realizó en 1984.

El equivalente en el Derecho Mexicano a la corporación norteamericana, es la sociedad anónima, que se rige por la Ley General de Sociedades Mercantiles, misma que tiene el carácter de ley federal, lo que permite establecer una primera diferencia con la regulación jurídica de las corporaciones, que como se ha dicho, es de carácter estatal.[6]

La sociedad anónima es una sociedad mercantil, que se constituye mediante escritura pública (artículos 5, 6 y 91 de la LGSM), bajo una denominación (artículo 87 LGSM) y compuesta exclusivamente de socios cuya obligación se limita al pago de sus acciones (artículo 87 LGSM).

La sociedad anónima, al igual que la corporación, es una entidad jurídica con personalidad distinta de la de sus socios (artículo 2º de la LGSM en relación con el artículo 25, fracción III, del Código Civil).

3. DERECHO CORPORATIVO Y DERECHO EMPRESARIAL

El estudio de la constitución, administración y regulación jurídica de las corporaciones, corresponde al Derecho Corporativo o Corporate Law, que no es una rama jurídica aislada, sino que se integra por diversas disciplinas tanto jurídicas como económicas, de entre las cuales sobresalen por su importancia, el derecho de valores y el derecho antimonopolios.

---

2 Idem. 9 de marzo de 2000.

3 Mantilla Molina, Roberto L. "Derecho Mercantil" Editorial Porrúa, México,1984, pág. 103.

4 Torres Charles, Sergio. "Fusiones y adquisiciones. Una Aproximación al Derecho de los Estados Unidos de América". Abril de 2000. http://www.foxware-mex.com/Articulos/articulos.html

5 Cheeseman, Hemry R. "Business Law. The Legal, Ethical and International Environment" Prentice Hall, 1992, Pág. 778.

6 Tanto México como los Estados Unidos son Estados federals cuyas leyes tienen dos ámbitos distintos de validez espacial. Las leyes federales promulgadas por el Congreso de la Unión, rigen en todo el territorio nacional, en tanto que las leyes locales o estatales, solamente rigen y se aplican en los Estados miembros de la federación cuyos Congresos las hayan publicado.

En los Estados Unidos se distingue entre corporaciones privadas y corporaciones públicas. Las corporaciones privadas no cotizan sus acciones al público, sino que éstas son propiedad de uno o varios accionistas, involucrados directamente con la administración de la corporación. Las corporaciones públicas, por el contrario, ofrecen sus acciones al público y los accionistas no tienen ingerencia en la administración corporativa.

La materia más relevante del Derecho Corporativo es la de fusiones y adquisiciones (mergers and acquisitions), que por su importancia para la economía nacional de los Estados Unidos, están reguladas tanto por leyes federales, como por leyes estatales.

La reglamentación jurídica de las fusiones y adquisiciones corporativas, se centra en dos aspectos fundamentales: uno, la regulación de la transferencia del control de la administración de las corporaciones, tanto desde el punto de vista de las leyes de corporaciones, como desde el punto de vista del mercado de valores y, dos, la regulación del control de un mercado relevante, adquirido por medio de un proceso de fusión o de adquisición (leyes antitrust).[7]

Si bien en México también existen leyes antimonopolios y del mercado de valores, no puede hablarse de que exista en realidad un "Derecho Corporativo Mexicano", en primer término, porque en nuestro país no existen corporaciones, sino sociedades anónimas, y en segundo lugar, porque tampoco existen los procesos de fusión y adquisición corporativas, tal como se conocen y reglamentan legalmente en los Estados Unidos.[8]

La LGSM, regula en sus artículos 222 a 227, el procedimiento de fusión de sociedades, pero no hace referencia alguna a las adquisiciones. Por su parte, la LMV, no contiene disposiciones relativas a la fusión de sociedades, ni tampoco a las de adquisiciones, sino que se limita a regular la oferta pública de valores y las actividades, personas y autoridades relacionadas con ella, sin incluir las operaciones tendientes a obtener el control de una sociedad.[9]

El estudio de las sociedades anónimas corresponde en México al Derecho Mercantil.[10] El estudio del mercado de valores y su regulación, corresponde al Derecho Bursátil[11] y podría hablarse de un Derecho Antimonopólico Mexicano en gestación, dada la promulgación relativamente reciente de la Ley Federal de Competencia Económica.[12]

Todas esas materias podrían quedar comprendidas en un Derecho Empresarial Mexicano, similar al Derecho Corporativo, por cuando a que agrupa diversas disciplinas atinentes al estudio amplísimo de la sociedad anónima.[13]

4. PODER E INFORMATICA.

Debemos distinguir entre el poder como facultad de gobernar una corporación, y la concentración de corporaciones como una forma de obtener poder económico y de mercado sobre los competidores.

Ambos casos se encuentran íntimamente ligados. La concentración de corporaciones mediante fusiones y adquisiciones, no puede llevarse a cabo sin la concurrencia del poder de decisión dentro de las empresas involucradas.

---

7 Torres Charles. Op. Cit.

8 Idem

9 El artículo 1º de la Ley del Mercado de Valores dice:

"Art. 1º.-La presente ley regula, en los términos de la misma, la oferta pública de valores, la intermediación en el mercado de éstos, las actividades de las personas que en él intervienen, el Registro Nacional de Valores e Intemediarios y las autoridades y servicios en materia de mercado de valores.

En la aplicación de la presente ley dichas autoridades deberán procurar el desarrollo equilibrado del mercado de valores y una sana competencia en el mismo."

10 El artículo 3, fracciónes II y III del Código de Comercio, reputa como comerciantes a las sociedades constituidas con arreglo a las leyes mercantiles y a las sociedades extranjeras o a sus agencias o sucursales que realicen actos de comercio en el territorio mexicano. El artículo 4º de la Ley General de Sociedades Mercantiles dispone que se reputarán mercantiles, todas las sociedades que se constituyan en alguna de las formas reconocidas en el artículo 1º de la propia ley.

11 Igartúa Araiza, Octavio. "Introducción al Estudio del Derecho Bursátil Mexicano". Editorial Porrúa, México, 1988. pp. 1 y ss.

12 La Ley Federal de Competencia Económica, fue promulgada el 24 de diciembre de 1992.

13 Torres Charles. Op. Cit.

En los Estados Unidos, tanto la obtención del poder para gobernar una corporación pública, como los procesos de fusiones y adquisiciones, se encuentran extensamente reglamentadas, en una esfera legal que gira alrededor de un eje fundamental: la "divulgación de información".

Como se verá más adelante, la Internet ha facilitado la consecución de los objetivos del principio de divulgación, propiciando cambios en las normas estadounidenses regulatorias de las fusiones y adquisiciones corporativas, así como en las disposiciones regulatorias del mercado de valores mexicano.

5. JOINT VENTURES

La tendencia actual en los Estados Unidos y en México, es la formación de alianzas estratégicas entre empresas nacionales o internacionales. Esas alianzas se verifican por dos vías: mediante joint ventures, o mediante adquisiciones.

Los contratos denominados de joint venture, son contratos de asociación entre dos o más corporaciones o sociedades que, sin llegar a constituir una nueva entidad se celebran para llevar a cabo negocios determinados.

La celebración de ese tipo de contratos es común en el ámbito internacional, en el cual ciertos países tienen restricciones políticas o legales, para que una empresa extranjera participe como inversionista en una compañía nacional. Entre los países industrializados, Japón restringe notablemente las inversiones foráneas a la celebración de joint ventures y en muchas ramas de la industria, un socio extranjero, solamente puede participar en un negocio como asociado minoritario.[14]

Los contratos joint venture se han incrementado con el uso de la Internet, pues existen firmas intermediarias especializadas, que ponen en contacto a los inversionistas con empresas interesadas en obtener capital, para llevar a cabo proyectos determinados sin involucrarse en procesos de fusión u otras formas de combinación formal de empresas.

6. ADQUISICIONES CORPORATIVAS

En los Estados Unidos las leyes de corporaciones, protegen al consejo de administración -board of directors- al concederles facultades para aprobar o reprobar fusiones, adquisiciones y otros actos relevantes en la vida de la corporación.

En México, esas facultades se encuentran reservadas a la Asamblea General Extraordinaria de los accionistas (artículos 181 y 182 de la LGSM), por lo que la tendencia de la legislación mexicana es la protección de los accionistas y no del órgano de administración social.

Partiendo de esa base, bajo el concepto general de "adquisición" en el Derecho Corporativo de los Estados Unidos, se comprenden los conceptos específicos de fusión; consolidación; adquisición de bienes corporativos e intercambio de acciones.

Esas figuras son procesos voluntarios mediante los cuales se logra la combinación de empresas, entendiéndose por "voluntarios", aquellos en los que el consejo de administración aprueba la operación de que se trate.

Existen sin embargo otros procesos, en los cuales una corporación obtiene el control de otra, en contra de la voluntad del consejo de administración de la adquirida. Esos procesos son denominados adquisiciones del control corporativo y comprenden los proxy contest, takeover contest y leveraged buyouts.[15]

---

[14] Corley, Robert N. y Reed, Lee O. "The Legal Environment of Business". Mc-Graw.Hill, 1987. pp 379-380.
[15] Torres Charles. Op. Cit.

Los procesos de adquisición no se encuentran regulados en el derecho mexicano, salvo cuando se trata de sociedades pertenecientes al sistema financiero;[16] los procesos de adquisición del control corporativo, son prácticamente desconocidos por las leyes mexicanas, aun cuando teóricamente pueden darse en la práctica.

6.1. Regulación del Mercado de Valores en los Estados Unidos.

Las fusiones y adquisiciones corporativas, no podrían comprenderse cabalmente sin una referencia, aunque sea somera, del mercado de valores de los Estados Unidos y su regulación jurídica, por lo que a continuación se hace un resumen sobre el origen de las leyes federales de valores y sus esquemas regulatorios.

En 1911, el Estado de Kansas aprobó la primera ley local sobre regulación de valores, conocida también como la "Blue Sky Law". El ejemplo de Kansas fue seguido por otros estados y pronto las "blue sky laws" comenzaron a surgir a través de los Estados Unidos, hasta el punto en que actualmente, todos los estados de la Unión Americana, tienen su propia legislación sobre valores.

No obstante las ventajas y el potencial de las blue sky laws, estas pronto demostraron ser inefectivas sobre todo tratándose de fraudes con valores en el ámbito nacional.

Como resultado del desastre de 1929, el Congreso promulgó la Securities Act of 1933 (Ley de Valores de 1933), conocida también como la "Truth in Securities Act".

Al tiempo de su promulgación, la ley de 1933 fue aplicada a través de la Federal Trade Comission (Comisión Federal de Comercio).

En 1934, el Congreso promulgó la Securities Exchange Act of 1934, que contiene una regulación más completa que la de su antecesora, pero tan vasta, que el Congreso consideró que no era posible continuar sobrecargando a la Federal Trade Comission con nuevas responsabilidades administrativas, y de esta forma creó la Securities and Exchange Comission (Comisión de Valores), una de las más grandes dependencias gubernamentales de los Estados Unidos de América, hoy en día.[17]

La Securities Exchange Act of 1934, regula todos los aspectos de la comercialización pública de valores. El aspecto medular de ley, en relación a la emisión de valores, se refiere a los requisitos de divulgación de información, derivados de la obligación de registrar ante la SEC, todos los valores operados en una bolsa de valores nacional.[18]

No obstante, dicha ley regula también otras actividades corporativas no necesariamente relacionadas con la emisión de valores. Una de ellas es la regulación del derecho de voto en todas las corporaciones que coticen sus acciones al público.

---

16 La Secretaría de Hacienda tiene facultades de autorizar la incorporación de una nueva sociedad a un grupo financiero ya constituido o bien la fusión de dos o más grupos, así como la fusión de dos o más entidades participantes en un mismo grupo; fusión de dos o más instituciones de banca múltiple, organizaciones auxiliares del crédito, casas de bosla, especialistas bursátiles, instituciones de fianzas e instituciones de seguros, en las quese incluye también la escisión.

Dichas facultades derivan de las siguientes disposiciones legales: artículo 10 de la Ley de Agrupaciones Financieras; artículo 27 de la Ley de Instituciones de Crédito; artículo 5º, fracción XI, 8º fracción III-2 y 67 de la Ley General de Organizaciones y Actividades Auxiliares del Crédito; 17 fracción VII de la Ley del Mercado de Valores; 15, fracción III y XI de la Ley Federal de Instituciones de Fianzas; 22 fracción II, 29 fracción X y 95 de la Ley General de Instituciones y Sociedades Mutualistas de Seguros.

Tratándose de casas de bolsa, también tiene intervención la Comisión Nacional Bancaria y de Valores, atento al contenido del artículo 19, fracción III de la Ley del Mercado de Valores.

17 Lee Hazen, Thomas. "The Law of Securities Regulation". West Publishing Co., 1990. pp. 7 y ss.

18 Los valores que cotizan publicamente en los Estados Unidos, son comercializados en mercados de valores formales y en mercados menos formales denominados over the-counter. Las más grandes y prestigiosas bolsas nacionales de valores son la New York Stock Exchange, seguida en tamaño y prestigio por la American Stock Exchange. Ambas bolsas son reconocidas y reguladas en la sección 6 de la Securities Exchange Act of 1934 y están sujetas a la supervisión de la Securities and Exchange Comision.

En 1968, el Congreso adicionó la ley con la Williams Act Amedments, la cual impone la obligación a los consejos de administración, de revelar información relativa a procesos de adquisición del control de corporaciones públicas.

6.2. Solicitud de Poderes y Regulación del Derecho de Voto.

En el derecho corporativo existe la figura denominada "solicitation of proxies", o solicitud de poderes, regulada por la Securities Exchange Act of 1934, figura que no tiene equivalente en el derecho mexicano de sociedades mercantiles, ni el el derecho bursátil.

En Estados Unidos los accionistas de una corporación, tienen el derecho de votar en la elección de consejeros, fusiones, enmiendas estatutarias y otros asuntos relativos al manejo de la empresa. Ese derecho de voto lo pueden ejercitar personalmente o a través de otra persona por virtud de un mandato.

El mandato o proxy, es un documento escrito por el accionista y dirigido a la corporación, por virtud del cual, se autoriza a otra persona, el "proxy holder", a votar por el accionista en las asambleas de la corporación.[19]

En México, el derecho de voto también puede ejercitarse a través de un mandatario (artículo 192 LGSM), pero está expresamente prohibido, que los administradores y comisarios de la sociedad puedan actuar como apoderados de un accionista en las asambleas de la sociedad.

Por el contrario, en los Estados Unidos, la mayor parte de las veces, el proxy holder es un miembro del consejo de administración u otro empleado administrativo de la corporación, que previamente a la celebración de una asamblea, ha solicitado a los accionistas que le confieran mandato para votar en su representación, en la elección de un candidato al consejo de administración o para aprobar o desaprobar proposiciones particulares hechas por otros administradores.[20]

La solicitud de poderes a los accionistas, es remitida por el interesado a cada accionista, conteniendo tanto una declaración como todo el material relativo a los asuntos en los cuales se ejercitará el derecho de voto. Dicha declaración es conocida como "proxy statement".

6.2.1. Regulación del Derecho de Voto bajo la Securities Exchange Act of 1934.

Al promulgarse la Securities Exchange Act en 1934, el Congreso tomó nota de que un gran número de fraudes corporativos, habían sido perpetrados por los administradores, a través de la solicitud de poderes a los accionistas, sin indicar a éstos la naturaleza de los asuntos respecto de los cuales se emitiría el voto.

Consecuentemente, la sección 14 de dicha ley, fue creada para regular los procesos de votación para las corporaciones que estan sujetas a los requisitos del registro de la sección 12, y a los requisitos de información de la sección 13 de la propia ley.[21]

La sección 14(a) de la Exchange Act, considera ilegal la solicitud de poderes en relación con cualquier valor registrado bajo la sección 12 de la misma ley, en contravención con las reglas que la SEC deba emitir.

En las reglas 14a-3 a 14a-12, emitidas por la SEC, se adopta el principio de "divulgación total" y se enumera la información que debe ser incluida en las solicitudes de poderes reguladas por la ley, por ejemplo:

---

19 Cheeseman. Op. Cit. Pág. 856.

20 Idem.

21 El texto de las leyes de valores de 1933 y 1934, puede consultarse en la siguiente dirección de internet: http://www.law.uc.edu/CCL/sld-toc.html

1. Si el poder es o no revocable, y en caso de serlo, la forma como debe revocarse.

2. Una descripción de la persona que hace la solicitud, incluyendo la identificación de la persona que la costea.

4. Información relativa a los intereses de los administradores, gerentes y participantes en las cuestiones que serán sujetas a votación.

5. Información detallada en relación a cualesquier fusión, consolidación o adquisición respecto de las cuales deba emitirse el voto.

6. Descripción de cualquier propiedad a ser adquirida o vendida y cuya operación requiera el voto de los accionistas.

7. Los motivos para cualquier proposición de enmienda al acta constitutiva, estatutos u otros documentos que requieran la aprobación de los accionistas.

6.3. Fusiones

La fusión tiene lugar cuando una corporación es absorbida por otra y deja de existir. La corporación fusionante se conoce como "surviving corporation", la corporación que cesa de existir se denomina "merged corporation". La corporación fusionante adquiere todos los derechos, privilegios, poderes, deberes legales, obligaciones y responsabilidades de la corporación fusionada.[22]

Una fusión ordinaria requiere: a) la aprobación del consejo de administración de cada corporación (MBCA 72) y, b) el voto afirmativo de la mayoría de las acciones con derecho a voto de cada corporación (MBCA 71), aunque algunos estados exigen una mayoría de dos terceras partes más que un voto de mayoría simple.

6.4. Consolidaciones

La consolidación tiene lugar cuando dos o más corporaciones se fusionan para formar una corporación completamente nueva. La nueva corporación es denominada "consolidated corporation" (MBCA 72) y su acta constitutiva reemplaza las actas de las corporaciones participantes.

Para que una consolidación tenga lugar, se requiere la aprobación de: a) el consejo de administración de cada corporación consolidante y, b) el voto afirmativo de la mayoría de las acciones con derecho a voto de cada corporación consolidante (MBCA 72 y 73).

Hoy en día, las consolidaciones son casi obsoletas porque generalmente resulta más ventajosa la supervivencia de una de las corporaciones participantes. La RMBCA no hace referencia alguna a las consolidaciones.[23]

6.5. Regulación de Valores de las Fusiones

Si alguna de las corporaciones que intervienen en una fusión, tienen sus acciones listadas en una bolsa de valores nacional, deben sujetarse a sus requisitos particulares.[24]

---

[22] Cheeseman. Op. Cit. Pág. 858.
[23] Idem.
[24] Vid supra. Nota 18.

En el periodo de 1985-1988, la SEC instauró una serie de procedimientos contra corporaciones, aduciendo una inadecuada revelación de las negociaciones de fusión. La Suprema Corte dió algunos lineamientos al respecto en Basic Inc. v. Levinson, 438 U.S. 224, 108 S. Ct. 978, 99 L.Ed.2d 194 (1988), requiriendo la develación de negociaciones materiales de fusión, tomando en consideración los hechos de la situación, como por ejemplo, el tamaño relativo de las corporaciones participantes.[25]

6.6. Las Fusiones en el Derecho Mexicano.

Las fusiones de sociedades mercantiles se encuentran reguladas en los artículos 221 a 226 de la LGSM.

Mediante la fusión, la ley permite que una sociedad anónima transmita íntegramente su patrimonio o cambie su personalidad jurídica, sin que para ello se requiera liquidar y disolver a la sociedad, ni se proceda a la constitución ordinaria de una nueva.

El estudio comparativo de los principios que rigen a las fusiones en los Estados Unidos y en México, permite concluir que en ambos países las fusiones se originan como un medio de concentración de empresas; que por medio de la fusión se transmite sin mayor formalidad el patrimonio social de las sociedades participantes a la sociedad subsistente o a la nueva sociedad, y que las fusiones pueden ser por absorción (Estados Unidos) o integración (México), o por la constitución de una nueva sociedad, consolidación (Estados Unidos) o fusión propiamente dicha (México).

Las fusiones de sociedades anónimas mexicanas que coticen sus acciones en la Bolsa Mexicana de Valores, se consideran, conforme a la circular 11-28 de la CNBV, eventos relevantes que deben ser divulgados en beneficio de los inversionistas.

6.7. Adquisición de Bienes Corporativos.

Hasta este punto nos hemos referido a las fusiones y consolidaciones como procedimientos formales. Sin embargo, las corporaciones pueden obtener los mismos resultados prácticos de una fusión con medios menos formales, particularmente mediante las adquisiciones de bienes "purchase of assets" o intercambio de acciones "stock exchange".

En los círculos legales estadounidenses, esas operaciones son conocidas como fusiones de hecho, en contraste con las fusiones y consolidaciones formales.

No obstante que el efecto práctico de una adquisición será fusionar una compañía con otra, la compañía adquirente, por lo general, no requiere obtener la aprobación de los accionistas.

En México la venta de bienes de una sociedad anónima queda sujeta a las disposiciones estatutarias (artículos 181 y 182 de la LGSM).

7. INTERCAMBIO DE ACCIONES.

Una corporación puede adquirir todas las acciones de otra a través de un intercambio de acciones. En un intercambio de acciones, ambas corporaciones conservan su existencia legal. Después del intercambio, una corporación -parent corporation- deviene como propietaria de otra -subsidiary corporation- (MBCA 72A).

El intercambio de acciones es utilizado la mayor parte de las veces, para crear compañías dominatrices (holding companys).

---

[25] Torres Charles. Op. Cit.

Para ser efectiva, un intercambio de acciones requiere la aprobación del consejo de administración de la compañía adquirente y la aprobación del consejo de administración y de los accionistas de la compañía subsidiaria (MBCA 72A y 73). Los accionistas de la compañía adquirente no necesitan aprobar la operación. Los accionistas disidentes de la corporacion subsidiaria, tienen el derecho de oposición (MBCA 80(a)(3).

En México es posible efectuar un intercambio de acciones, quedando sujeto a las disposiciones estatutarias (artículos 181 y 182 de la LGSM).

8. ADQUISICIONES DEL CONTROL CORPORATIVO.

Los procedimientos para obtener la transferencia involuntaria del control de una corporación, son los siguientes, en orden de aparición histórica: 1) proxy contest (contiendas por los poderes; 2) takeover contest (compra de acciones) y 3) leveraged buyout (compras apalancadas)[26]

8.1. Proxy Contest.

Cuando los accionistas se oponen a las acciones tomadas por los titulares del consejo de administración de la corporación, pueden desafiarlo en un proxy contest en el cual ambas partes solicitan poderes de otros accionistas. *El lado que recibe el mayor número de poderes de los accionistas, ganará el proxy contest. Dichas contiendas se* presentan generalmente en relación a la elección de consejeros.

Las contiendas por poderes se asemejan a las campañas políticas. Los administradores titulares tienen su propio equipo de candidatos para ocupar el consejo de administración, en tanto que los socios insurgentes, ofrecen un equipo rival.

Los insurgentes aducirán, por lo general, que los administradores han equivocado el rumbo y prometen hacerlo mejor. Los titulares, por su parte, sostedrán que se han desempeñado adecuadamente, especialmente al lidiar con las circunstancias económicas, y aseguraran que las promesas de sus rivales no tienen sustento real.[27]

8.2. Tender Offer.

Un método frecuente para obtener la combinación de dos corporaciones, es la venta de las acciones de una a otra. Esta operación generalmente se completa por el consejo de administración de la compañía adquirente, sin necesidad de la aprobación de los accionistas.

A menos que la compra sea hecha con propósitos de inversión solamente, la meta de la compradora, obviamente, será la obtención del número suficiente de acciones para controlar la compañía cuyas acciones se adquieren. El control requiere usualmente la propiedad de más del 50 por ciento de las acciones con derecho a voto.

A pesar de que la aprobación del consejo de administración no es un requisito legal para la adquisición de acciones de la corporación a adquirir, dicho consejo puede encontrarse en la posición de entorpecer la compra de acciones en el mercado abierto, si se opone al cambio de control.

En virtud de que en muchas ocasiones la corporación adquirente precisa movimientos rápidos, frente a la oposición del consejo de administración de la compañía por adquirir, puede entonces hacer una oferta de compra directamente a los accionistas.

---

26 *Idem.*

27 Williamson E., Robinson. "Mergers, acquisitions, and leveraged buyouts: an efficiency assessment. En Corporate Law and Economic Analysis. Cambridge University Press, 1991. Pág. 8.

Dicha oferta se conoce como "tender offer" y a la compañía cuyas acciones se pretende adquirir, se le conoce como "target corporation" (corporación objetivo)[28]

La tender offer es una oferta pública hecha a los accionistas de la corporación objetivo, para comprar a un precio especifico, aquellas acciones disponibles.

La oferta también es conocida como "takeover bid" y las adquisiciones de acciónes se conocen como "takeovers".

La ventaja principal de una tender offer es la velocidad. La compañía adquirente probablemente obtendria suficientes acciones para tomar el control, antes que el consejo de administración de la compañía objetivo pudiera erigir barreras efectivas para evitar la adquisición.

A pesar de que el precio a pagar se ofrece por lo general en efectivo, puede consistir también en un número determinado de acciones de la compañía adquirente por cada acción de la compañía objetivo, o una combinación de dinero y acciones. El precio especificado puede también tomar la forma de bonos u otras propiedades de la compañía adquirente, o una combinación de éstas con dinero.[29]

En una tender offer, la corporación oferente y la corporación objetivo, conservan su estatus legal. Una tender offer triunfante, es seguida algunas veces, por una fusión de las corporaciones.

8.3. Contiendas por el Control Corporativo -Takeovers-

Cuando una corporación intenta adquirir el control de las acciones de otra corporación, el consejo de administración de la compañía objetivo ocupa un papel central. Algunas veces dicho consejo verá a la tender offer favorablemente y recomendará a los accionistas que vendan sus acciones. Sin embargo, en la mayor parte de las situaciones, el consejo de administración de la corporación objetivo, resistirá los intentos de takeover y tratará de impedir la compra.

Una tender offer que es resistida por el consejo de administración es conocida como "hostil tender offer" o "unfriendly tender offer"[30]

La intensidad con la que son peleadas las batallas de takeover, se ilustra por la jerga que se ha desarrollado para denotar varias tácticas, tanto ofensivas como defensivas, adoptadas por las partes.[31]

Por ejemplo, los agresores pueden utilizar el elemento sorpresa a través de una oferta rapidamente implementada, conocida como "midnight special" -especial de media noche.

"Bear hug", abrazo del oso, se refiere a una aproximación inicial amistosa a la adminstración de la compañía objetivo, con la intención implícita o explicita, de acercarla tranquilamente o de arrastrarla posteriormente.

"White Knights", caballeros blancos, son corporaciones llevadas por la compañía objetivo para mantener a raya a los oferentes, mediante una mejora de la oferta; "Grey Knights", caballeros grises, son, por lo contrario, oferentes competidores, cuya ayuda no ha sido solicitada por la compañía objetivo, pero que son preferidos a los agresores iniciales; "Black Knights", caballeros negros, son oferentes competidores menos atractivos que los agresores iniciales.

La lista de heridos "wounded list", se refiere a los ejecutivos que han perdido sus trabajos o su salud, durante el curso de una campaña de takeover. Los takeovers también pueden involucrar tiroteos "shootouts" y a la larga, alguna resolución a través de pistoleros "hired guns", es decir, abogados.

---

28 Howell A. Rate, et al. "Business Law". Dryden Press, 1989, pág. 691.
29 Idem
30 Cheeseman. Op. Cit. Pág. 864.
31 Torres Charles. Op. Cit.

Adicionalmente a las tácticas defensivas, para ahorcar takeovers hostiles, nuevos y coloridos términos son acuñados. Por ejemplo, la defensa Pac-Man, la cual consiste en que la compañía objetivo, pasa a ser la compañía predadora y adquiere a su oferente.

8.4. Leveraged Buyouts

Las LBO's son una forma particular de transferir el control. Una compra apalancada -leveraged buyout- consiste en financiar una parte del precio de adquisición de una corporación, mediante el uso de deuda. El financiamiento se obtiene mediante la emisión y colocación de bonos conocidos como "junk bonds".

Los bonos corporativos, a diferencia de los bonos gubernamentales, tienen un riesgo crediticio real, en virtud de que el gobierno no los garantiza. Por lo mismo, las corporaciones pagan intereses que reflejan su crédito o el riesgo. Este último, es medido por agencias como Standard & Poor's y Moody's.[32]

En general, un junk bond es un bono calificado muy bajo en el índice Standard and Poors, usualmente bien abajo del grado de inversión confiable.

9. INFLUENCIA DE LA INTERNET EN LA REGULACION DE ADQUISICIONES CORPORATIVAS.

En octubre 22 de 1999, la SEC emitió nuevas reglas bajo la Securities Exchange Act of 1934, mismas que entraron en vigor el 24 de enero del año 2000.[33]

La SEC efectuó una revisión completa de las reglas y normas aplicables a las transacciones de takeover, incluyendo proxys, tender offers, fusiones, adquisiciones y transacciones extraordinarias similares. Las reglas revisadas, según la SEC, permitirán el incremento de las comunicaciones entre los mercados y los tenedores de valores. Las reformas también balancearan el tratamiento de tender offers de dinero y acciones; simplificarán y centralizaran los requisitos de revelación de información y eliminarán las inconsistencias regulatorias en fusiones y tender offers.

Resulta interesante el hecho de que la emisión de las reglas aludidas, tuvo su origen en los cambios tecnológicos, concretamente, en el papel de la Internet en el mercado.

Como se expuso anteriormente, el derecho corporativo y de valores de los Estados Unidos, gira alrededor del eje de "divulgación de información" a los accionistas de una corporación, que deban emitir su voto en relación a *procesos de solicitudes de poderes, o de fusiones y adquisiciones corporativas.*

Ese principio de divulgación, implica que el consejo de administración de la corporación interesada, debe remitir por correo todo el material relativo a las decisiones que se tomarán en una asamblea de accionistas, sin ocultar ni falsear la información, bajo la pena de nulificar los acuerdos y de sanciones criminales para los administradores responsables.

Es así que conforme a las antiguas, pero todavía vigentes reglas de la SEC, los consejos de administración de corporaciones involucradas en procesos de proxy o de adquisiciones corporativas, deben presentar preliminarmente ante dicha dependencia, prospectos, declaraciones de proxy, o declaraciones de tender offer conteniendo información completa y balanceada, antes de solicitar a los accionistas la emisión de su voto sobre una decisión de inversión.

Una vez que todo el material divulgatorio está preparado para su remisión a los accionistas en forma definitiva, los administradores tienen obligación de presentarlo nuevamente ante la SEC, por lo menos dos días antes de la asamblea y, simultáneamente deben presentarlo ante las bolsas de valores nacionales en donde la corporación tenga listadas sus acciones.

---

[32] *Idem.*

[33] Regulation of Takeovers and Security Holder Communications. October 26, 1999. Effective date: January 24, 2000. [Release No. 33-7760; 34-42055; File No. S7-28-98] (File name: 33-7760.htm) http://www.sec.gov/rules/finrindx.htm

Hasta antes del uso generalizado de Internet, los procesos de divulgación de la información a través del correo eran lentos, sobre todo porque los tenedores de valores de una corporación pública, generalmente están diseminados por todo el país y aun en el extranjero. Sin embargo, a raíz de que la Internet se popularizó, las reglas del juego cambiaron y la SEC tuvo que adecuar sus normas regulatorias al nuevo esquema del mercado.

La SEC consideró que las transacciones de fusiones y adquisiciones están ocurriendo actualmente a un ritmo más rápido, en virtud del desarrollo de nuevas tecnologías y del avance en las comunicaciones (Internet). Como resultado de las presiones económicas y regulatorias, muchas compañías liberan más información al mercado antes de que una declaración obligatoria sea presentada a la SEC.

La Comisión reconoció que la restricción a las comunicaciones tempranas, derivadas de diversos ordenamientos jurídicos, pueden actualmente impedir, más que promover, inversiones informadas y decisiones de voto.

Sobre tal base, la Comisión adoptó reglas proxy y reglas tender offer que permiten las comunicaciones por un período irrestricto, considerando que uno de los mayores beneficios de permitir las comunicaciones tempranas, es que mayor cantidad de información estará disponible para todos los tenedores de valores, y no simplemente limitada a una audiencia de analistas financieros.

10.- DIVULGACION DE INFORMACION A LOS ACCIONISTAS DE SOCIEDADES ANONIMAS EN MEXICO.

Si bien es cierto que las leyes mexicanas, no regulan los procesos de adquisiciones corporativas, no por ello ha dejado de sentirse la influencia tanto del Derecho Corporativo, como de la Internet, en el mercado de valores mexicano.

La Comisión Nacional Bancaria y de Valores, siguiendo el principio del Derecho Corporativo de "divulgación de información", emitió la circular 11-28, en la que consideró que la divulgación oportuna de información relativa a eventos capaces de influir en los precios de los valores que son materia de intermediación en el mercado, es condición necesaria para dar mayor certidumbre e igualdad para la toma de decisiones de inversión.[34]

Bajo ese supuesto, la Comisión estimó conveniente incorporar a los medios electrónicos en la difusión de los actos, hechos o acontecimientos que constituyen los citados eventos relevantes, a fin de contar con vías expeditas para su revelación pública, por lo que impuso la obligación a las emisoras, de determinar bajo su responsabilidad, la información sobre eventos relevantes que harán pública, así como, en su caso, aquélla cuya revelación habrán de diferir.

En la disposición segunda de la circular, la Comisión dispuso que en caso que las emisoras opten por diferir la revelación de algún evento relevante, deberán adoptar las medidas necesarias para garantizar que la información relativa sea conocida por el menor número posible de personas y llevar un registro con los nombres de tales personas, que incluya la fecha y hora en que se hicieron conocedores de la información, obteniendo de las mismas un compromiso de confidencialidad, conservando dicha información el carácter de privilegiada para todos los efectos legales aplicables.

La información sobre eventos relevantes no podrá ser objeto de diferimiento cuando se trate de actos o hechos consumados, o bien, cuando se presenten movimientos inusitados de los valores en el mercado que estén relacionados con dicha información, en cuyo supuesto las Emisoras deberán revelar la información inmediatamente.

Para efectos de lo dispuesto en la Circular, se entiende por movimiento inusitado, cualquier cambio en la oferta o demanda de los valores o en su precio, que no sea consistente con su comportamiento histórico y no pueda explicarse con la información que sea del dominio público.

[34] La circular puede ser consultada en el sitio de la Comisión Nacional Bancaria y de Valores en la siguiente dirección: http://cnbv.gob.mx/index.htm

Por otra parte, el Reglamento de la Bolsa Mexicana de Valores, en su título noveno, regula la forma como las emisoras deben proporcionar la información para su divulgación entre el público inversionista. Resulta de particular relevancia, el hecho de que toda la información que se proporcione a la bolsa, se verifica a través Emisnet, sistema electrónico de la Bolsa que, a través de una red de comunicación, permite la transmisión de información al público en general, a la Bolsa y a la Comisión, cuando así lo requiera el propio Reglamento.[35]

La regla 9.005.00 del reglamento, dispone que se considera información pública aquélla que de acuerdo con las Disposiciones aplicables, deba mantenerse y, en su caso, divulgarse entre el público en general a través de los medios a los que se refiere el Título Noveno, incluyendo los Indicadores de Mercado.

La regla 9.008.00 preceptúa que la Bolsa hará publicaciones y tendrá a disposición del público, respecto de las Operaciones del mercado de capitales de manera enunciativa mas no limitativa, la siguiente información:

I. Cotizaciones.

II. Indicadores de Mercado y estadísticas.

III. Desglose de Operaciones y operatividad por miembro.

IV. Información jurídica, financiera y contable de las Emisoras.

V. Incumplimientos de las Emisoras respecto de sus obligaciones de pago.

VI. Avisos de interés para el mercado.

La regla 9.011.00, se refiere a que la Bolsa podrá hacer publicaciones periódicas en medios impresos o electrónicos, las cuales se editarán con la frecuencia que determine la Bolsa, con base en las características de la información que se pretenda difundir.

En cumplimiento a las reglas 9.008.00 y 9.011.00 y a la circular 11-28 de la Comisión Nacional Bancaria y de Valores, la Bolsa Mexicana de Valores mantiene un sitio en la Internet en el que informa no solamente el comportamiento del mercado, sino los eventos relevantes de las emisoras.[36]

Resulta interesante resaltar el hecho de que la circular 11-28 de la CNBV, se emitió en el año de 1997. Lo anterior nos lleva a concluir que si bien es cierto que la Comisión adoptó hasta finales del siglo XX el principio de "divulgación de información", que durante años ha sido el pilar del mercado de valores norteamericano, también lo es que se anticipó dos años a su símil norteamericana, al reconocer el papel decisivo de la Internet, en la divulgación de información relevante para los accionistas.

35 *El reglamento puede consultarse en el sitio de la Bolsa Mexicana de Valores, en la siguiente dirección:* http://bmv.com.mx/bmv/reglamentobmv.html

36 http://bmv.com.mx

Derecho Empresarial Informático en Internet y el uso de la Microforma Digital

Julio Núñez Ponce (Perú)

Abogado, Catedrático de Derecho Informático en la Universidad de Lima Magister en Derecho Empresarial. Presidente de la Asociación de Fedatarios Juramentados con Especialización en Informática (AFEJESI-RED). Miembro del Comité Organizador del VII Congreso Iberoamericano de Derecho e Informática. Doctorando en Derecho. Autor de los libros : Derecho Informático (1996) y Software : Licencia de Uso, Derecho y Empresa (1998).

1. INTRODUCCION

1.1. Aspectos Generales

El Derecho Empresarial incluye los aspectos relativos a la empresa como centro de imputación jurídica y a nuestro parecer debe incluir también los problemas relativos a la informática con incidencia empresarial dando origen al Derecho Informático Empresarial o al Derecho Empresarial Informático.

En este campo del Derecho Empresarial informático el tema de la Contratación Electrónica en Internet y el comercio electrónico en general están teniendo gran desarrollo en nuestros países ; conjuntamente, a este crecimiento se plantea el problema de la seguridad tanto en el envío del mensaje como en la autenticación del contenido del mensaje. En nuestro país, se ha avanzado legislativamente en esta materia.

En efecto, en el Perú, conforme el artículo 13º del Decreto Legislativo 681, modificado por la Ley 26612 , se establece que "las microformas en la modalidad de documentos informáticos, los microduplicados y sus copias fieles pueden ser utilizados en la transferencia electrónica de fondos, en la transferencia electrónica de datos informatizados (EDI) y otros servicios de valor añadido, conservando para todos sus efectos legales su valor probatorio". En la legislación peruana los servicios de valor añadido incluyen Internet. Por otra parte, El sistema de microformas en la modalidad de documentos informáticos requiere el cumplimiento de requisitos formales y técnicos ; como requisito formal se establece que los procesos de micrograbación sean autenticados por fedatarios juramentados o por notarios públicos. Por consiguiente en el tema de la contratación electrónica y de la firma digital, va a tener participación activa el fedatario juramentado.

El objetivo de la presente ponencia es vincular el tema del Derecho Empresarial Informático con el tema del uso de la microforma digital en su incidencia empresarial en temas tributarios, societarios, de competencia deslela entre otros, la función del fedatario juramentado que realiza fe pública informática y la actividad en Internet, conforme la legislación peruana .

1.2. La Contratación Electrónica y la Seguridad en la Red

"Entendemos por contratación electrónica aquella que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo"[1].

El explosivo crecimiento de los sistemas de computación y sus interconexiones a través de redes ha aumentado la dependencia de organizaciones y particulares en la información guardada y comunicada por medio de estos sistemas. Ello ha conducido a una mayor preocupación por proteger datos y recursos, a garantizar la autenticidad de los datos y mensajes, y a proteger los sistemas contra posibles ataques.

[1] DAVARA RODRIGUEZ, Miguel Angel : "Manual de Derecho Informático". Editorial. Aranzandi. Pamplona, España. 1997. Pág.165.

Los requerimientos de Information Security en el ámbito de las organizaciones han sufrido dos cambios radicales en las últimas décadas. Antes de la utilización masiva de los equipos de procesamiento de datos, la seguridad de información considerada valiosa por una organización se obtenía fundamentalmente a través de medios físicos (archivos bajo llave) y administrativos. Con la aparición de las computadoras resultó evidente la necesidad de herramientas automáticas que protegieran los datos y otra información guardada en aquellas. El nombre genérico dado a la colección de herramientas desarrolladas para la protección de datos es el de Computer Security.

El segundo cambio que afecta la seguridad es la aparición de redes y otras facilidades de comunicación para el transporte de datos. "Se necesitan medidas de Network Security para proteger los datos durante su transmisión. En realidad, el término network security puede llevar a engaño, dado que las organizaciones comerciales, gubernamentales y académicas interconectan sus equipos de procesamiento de datos con una serie de redes a su vez interconectadas. De allí que se hable de Internetwork Security.

"Se define a la Internetwork Security como "las medidas para determinar, prevenir, detectar y corregir violaciones de seguridad relacionadas con la transmisión de información"[2]

1.3. El Comercio en Internet.

El comercio electrónico en Internet es uno de los aspectos más relevantes del desarrollo de la red de redes, al permitir que particulares y empresas alcancen la globalidad , con un costo reducido, apertura de mercados, posibilidad de eficaz gestión de recursos e inventarios. Frente a esta perspectiva de crecimiento las sociedades de medios de pago e instituciones financieras deben establecer especificaciones abiertas que permitan : proporcionar confidenciabilidad en los mensajes de datos ; autentificar la identidad de las partes ; garantizar la integridad de las instrucciones de pago.

Si bien la contratación electrónica ofrece grandes ventajas tales como la reducción de costos para las empresas, la falta de necesidad de un espacio físico para las ventas, la reducción de personal, esto a la vez podría llegar a traer ciertos problemas que deberían ser tomados en cuenta. Uno de estos problemas es la seguridad en la contratación debido a que los pagos se hacen a través de tarjetas de crédito cuyos números podrían ser conocidos por cualquiera. Frente a ello se están desarrollando sistemas de seguridad y directivas que se orientan a esta finalidad. Por ejemplo, quienes realizan transacciones a través de la vasta Red Mundial cuentan con nuevas directrices emitidas por la Cámara de Comercio Internacional (CCI) que tienen la finalidad de dar mayor confiabilidad a sus negocios. Este conjunto de normas conocido como GUIDEC (GENERAL Usage in International Digitally Ensured Commerece), han sido diseñadas por expertos de los más importantes suministradores de software de internet, profesionales legales, autoridades de certificación y bancos comerciales.

Las GUIDEC no sólo regulan el uso de una criptografía clave pública para las firmas digitales, sino que establecen los procedimientos para certificar transacciones calificadas como "mensajes seguros", si es que existen dudas de hacer negocios con un socio que aparece en Internet. Esta certificación se llevaría a cabo a través de una tercera parte confiable llamada "certificador" que asegure que los poseedores de claves públicas sean quienes ellos dicen que son. Estas directrices, que significan un paso crucial para la autoregulación del comercio electrónico, fueron lanzadas por la CCI en la Conferencia Internacional "Agenda del Mundo Empresarial para el Comercio Electrónico", y serán actualizadas de acuerdo con los desarrollos de la tecnología digital.

2. LA MICROFORMA DIGITAL Y EL DERECHO EMPRESARIAL INFORMATICO

2.1. Marco Legal de la Microforma Digital en el Perú.

El Decreto Legislativo 681 publicado en el Diario Oficial "El Peruano" en Octubre de 1,991 y vigente desde

2" La Seguridad en la Red". URL : http://www.it-cenit.org.ar/Publicac/ReflexSEG/Reflex1.html

Noviembre del mismo año, en sus considerandos establece " que es conveniente ... regular el uso de tecnologías avanzadas en materia de archivo de documentos e información... respecto a la .. producida por procedimientos informáticos en computadoras.." . Esta norma regula el valor probatorio y los efectos legales tanto del microfilm como del documento informático que los incluye dentro del concepto de microforma; en esta ponencia vamos a referirnos específicamente al documento informático.

El artículo 1º del Decreto Legislativo 681, modificado por la Ley 26612, define a la microforma como "imagen.. compactada o digitalizada de un documento, que se encuentra grabada en un medio físico técnicamente idóneo, que le sirve de soporte material portador, mediante un proceso .. informático, electrónico, electromagnético o que emplee alguna otra tecnología de efectos equivalentes, de modo que tal imagen se conserve y pueda ser vista y leída con la ayuda de equipos visores, pantallas de video o métodos análogos; y pueda ser reproducida en copias impresas esencialmente iguales al documento original" y define al microduplicado como "reproducción exacta o copia del elemento original que contiene microformas , efectuada sobre un soporte material similar, en el mismo tamaño y formato; y con efectos equivalentes". El artículo 2º , precisa que se rigen por esta ley los efectos legales y el mérito probatorio de las microformas, de las copias fieles autenticadas de ellas y de sus microduplicados, siempre que en su preparación se cumplan los requisitos prescritos que son de orden formal y técnico.

Como requisito formal, se establece que los procesos de micrograbación ,que son aquellos por los cuales se obtienen la microformas, sean autenticados por fedatario o por Notario Público. Para ser fedatario juramentado se requiere:

- Reunir las condiciones exigibles para postular a la plaza de notario público y acreditarlo ante el Colegio de Abogados de la jurisdicción. Para ello basta con presentar al Colegio de Abogados documentación acreditando que el solicitante esta apto conforme a ley para presentarse a postular a una plaza notarial (es decir que sea abogado y cumpla los demás requisitos).

- Haber obtenido el diploma de idoneidad técnica, este diploma con carácter oficial puede ser expedido por el Colegio de Abogados que para este efecto está facultado para organizar cursos de capacitación a cargo de expertos o técnicos en la materia. Para este fin el Colegio de Abogados puede coordinar y celebrar convenios de cooperación con personas expertas en estas tecnologías y con universidades. Esta capacitación deberá ser cumplida en forma constante por los fedatarios públicos o privados y generará el puntaje que precise el reglamento, para efectos de su ratificación cada cinco años. La ratificación será realizada por el Colegio de abogados y/o notarios que emitió el certificado de idoneidad técnica, previa evaluación académica, conforme el procedimiento precisado en el reglamento.

- Inscribirse y registrar su firma en el Colegio de Abogados de su jurisdicción y prestar juramento ante el Presidente de la Corte Superior.

Conforme al reglamento, el único requisito exigido a los notarios para que puedan autenticar la obtención de microformas en la modalidad de documentos informáticos es que deben haber obtenido el diploma de idoneidad técnica y hacerlo registrar en el Colegio Notarial.

Cómo requisito técnico se señala que los procedimientos que utilize (con un adecuado hardware y software en el presente caso) empleados en la confección de las microformas , sus microduplicados y copias fieles deben garantizar los resultados siguientes:

a) Que las microformas reproducen los documentos originales con absoluta fidelidad e integridad.

b) Que las microformas obtenidas poseen cualidades de durabilidad , inalterabilidad y fijeza superiores o al menos similares a los documentos originales.

c) Que los microduplicados sean reproducciones de contenido exactamente igual a las microformas originales y con similares características.

d) Que a partir de las microformas y de los microduplicados pueda recuperarse , en papel u otro material similar, copias fieles y exactas del documento original que se halla micrograbado en aquellos.

e) Que las microformas bajo la modalidad de documentos producidos por procedimientos informáticos y medios similares tengan sistemas de seguridad de datos e información que aseguren su inalterabilidad e integridad. Asimismo, cuando en esta modalidad de microformas se incluya signatura o firma informática, ésta deberá ser inalterable, fija, durable y comprobable su autenticidad en forma indubitable; esta comprobación deberá realizarse por medios técnicos idóneos.

La aprobación de la infraestructura y equipo técnico adecuado (hardware,software y otros) según el Decreto Legislativo 681 y normas jurídicas complementarias está a cargo del Instituto de Defensa de la Libre Competencia y de la Propiedad Intelectual (INDECOPI). El artículo 26º del Decreto Legislativo 681º, modificado por la Ley 26612 dispone que " corresponde, adicionalmente a la Comisión de Reglamentos Técnicos y Comerciales, aprobar las normas técnicas para los equipos, software u otros medios que se utilicen para el proceso de micrograbación para la obtención de microformas tanto en la modalidad de microfilm como del documento informático, así como otorgar certificados de cumplimiento de estas normas y de idoneidad técnica a quien acredite contar con los medios técnicos adecuados; de conformidad con el Decreto Legislativo Nº 681, normas modificatorias y complementarias".

Frente a esta realidad normativa peruana, conviene tener en cuenta antecedentes jurídicos europeos que consideramos pueden haber intervenido en su dación. En la Recomendación R(81)20 del Consejo de Europa , sobre armonización de legislaciones que tiene como objeto , entre otros, la admisibilidad de las reproducciones en microfilm y en soporte informático como medios de prueba en un proceso existen disposiciones sobre esta materia, por ejemplo, el artículo 5º se ocupa específicamente de los documentos registrados en soporte informático , en general, y de los programas de computación y documentos informáticos , en especial, previendo la adopción de medidas que garanticen la inalterabilidad , permanencia y la posibilidad de reproducir en forma legible el documento informático en cualquier momento.

La Recomendación citada del Consejo de Europa ha sido puesta en práctica en Luxemburgo, mediante la ley de 22 de Diciembre de 1,986 y el decreto graduncal de igual fecha , por lo que se reformaron entre otros, el artículo 1348 del Código Civil y el 11 de Comercio, ambos de Luxemburgo. " La nueva regulación transpone el artículo 5º de la Recomendación y admite el valor probatorio de los registros informáticos hechos a partir del original de un documento privado bajo la responsabilidad del que tiene a su cargo el documento. Reconoce a estos registros en soporte informático el mismo valor que los documentos privados de los que se presume, salvo prueba en contrario, que son reproducción o registro fiel, pero solamente cuando los originales han sido detruídos dentro del marco de un método de gestión regularmente seguido y si responden a las condiciones que al efecto ha previsto el decreto graduncal" [3]. Esta regulación de Luxemburgo tiene elementos comunes con la legislación peruana contenida en el Decreto Legislativo 681º, con lo cual podemos afirmar que en su dación se ha tenido en cuenta la normatividad existente en el derecho comparado, especialmente en el ámbito europeo, pero también los avances en estas materias en el ámbito latinoamericano.

Conforme el Decreto Legislativo 681 los documentos informáticos contenidos en las microformas, que han sido obtenidos cumpliendo los requisitos formales y técnicos ya señalados, sustituyen a los expedientes y documentos originales micrograbados en aquellos, para todos los efectos legales. En consecuencia, los documentos informáticos contenidos en las microformas que en su proceso de micrograbación se ha cumplido los requisitos señalados, conforme los artículos 9º,10º,11º,13º del Decreto Legislativo 681 , tienen los siguientes efectos legales y valor probatorio:

i) Pueden ser utilizados en procesos judiciales o fuera de ellos. En el caso de utilizarse firmas digitales, deberá ser comprobable su autenticidad en forma indubitable. Una forma de comprobación

[3] HEREDEROS HIGUERAS, Manuel: " Valor Probatorio de los documentos electrónicos". En Encuentros sobre Informática y Derecho en la Universidad Pontificia Comillas de Madrid 1990-1991. Ed.Aranzandi 1992, Madrid, España, pág. 23

podría ser la autenticación o certificación del fedatario juramentado o del notario al momento de su emisión. Lo que daría mayor certeza al juez al evaluar esta prueba.

ii) Las copias autenticadas de las microformas de instrumentos privados son idóneas para el reconocimiento judicial de su contenido y firma, con los mismos procedimientos y alcances que los documentos originales. Lo que implica, que las firmas digitales pueden ser reconocidas en un proceso judicial.

iii) Las copias autenticadas no sustituyen a los títulos valores originales para el efecto de despachar ejecución o de exigir la prestación incorporada en el título . En caso de pérdida, extravío, deterioro o destrucción de original, una vez cumplidos los trámites legales para la expedición del duplicado, el juez toma en cuenta la copia autenticada de la microforma del título, para establecer el contenido del duplicado que se expida. Al respecto, cabe señalar que el proyecto de ley peruana de títulos valores está orientada a ser una ley de valores mobiliarios, que reconozcan los valores electrónicos. En efecto, se conoce que cuando el valor se expresa en un certificado o título, a él se denomina título-valor, cuando se representa mediante un golpe electromagnético o electrónico se le llaman valores electrónicos, entre los que están las anotación en cuenta", estos valores son incluidos en este proyecto de ley. Por consiguiente las microformas podrán , en caso de promulgarse este proyecto, contener títulos valores con mérito ejecutivo e incluirse firmas digitales para estos efectos.

Los microarchivos y los documentos contenidos en ellos son válidos para cualquier revisión de orden contable o tributario, así como para exámenes y auditorías , públicas o privadas. Pueden ser exhibidos ante los inspectores , revisores, auditores y autoridades competentes , directamente mediante su presentación en pantalla o aparatos visores, sin requerirse copia en papel , salvo que tengan que ser presentados los documentos en algún expediente o en caso similar. Bastará que se cumplan los requisitos técnicos y formales, incluso si se trata de documentos materia de contratación electrónica dentro del comercio en Internet.

Las microformas, los microduplicados y los documentos contenidos en ellos pueden ser utilizados en la transferencia electrónica de fondos, en la transferencia electrónica de datos informatizados (EDI) y otros servicios de valor añadido, conservando para todos sus efectos legales su valor probatorio. Debe tenerse en cuenta, que dentro de los servicios de valor añadido están incluidos también el comercio electrónico en Internet.

Las microformas pueden ser utilizadas a elección del empleador, para el cumplimiento de la obligación de llevar planillas de pago, conforme el reglamento respectivo[4]. El empleador que opte por llevar sus planillas en microformas será responsable de proporcionar los equipos y sistemas idóneos, a fin de que la Autoridad Administrativa de Trabajo o la autoridad competente, de requerirlo, puedan revisar el contenido de las planillas. Este sistema podrá utilizarse , previa adecuación normativa, al teletrabajo, permitiendo que los contratos de trabajo en Internet puedan tener registradas las planillas en microformas en la modalidad de documentos informáticos.

2.2. La Función del Fedatario Juramentado con Especialización en Informática.

La objetividad e integridad del Fedatario Juramentado es fundamental, debiendo en su condición de profesional del Derecho encargado de dar fe pública en los procesos y certificaciones reguladas por ley actuar en concordancia con los principios de honorabilidad, imparcialidad, veracidad y objetividad.

La función de los depositarios de la fe pública contemplados en el Decreto Legislativo 681, entendida como el conjunto de atribuciones que las normas les asignan, tiene como contenido principal la dación de fe pública. Esta es una atribución central, alrededor del cual giran otras que coadyuvan a lograr su objetivo (asesoramiento, dirección, archivo, etc). "La función de tales personas es compleja... dicha función reúne las características que tiene la función notarial, a saber :

Es legal : pues se ejerce a partir de normas expresamente sancionadas por el Estado.

[4] Reglamento de Planillas de Pago, aprobado por Decreto Supremo Nº 001-98-TR, publicado el 22 de Enero de 1998.

Es Jurídica : por razón de la materia que comprende su función:

Es pública : porque la autoridad que ella implica está contrapuesta al orden privado.

Sin embargo, adicionalmente en dicha función encontramos características exclusivas derivadas de la naturaleza del objeto sobre el cual recae, y que son :

Es altamente especializada : atañe al ámbito informático del Derecho (Derecho Informático).

Es técnica : atañe a complejos procesos tecnológicos, que requieren conocimientos extrajurídicos.

Su función en el marco de la contratación electrónica, previa adecuación legislativa, puede incluir además de autenticar los procesos de micrograbación, responsabilidades similares a que tienen las autoridades certificadoras en el caso de las firmas digitales.

La formación del Fedatario Juramentado con especialización en Informática y los Colegios de Abogados.

En el Perú los primeros Fedatarios Juramentados con especialización en Informática son profesionales abogados que han obtenido sus respectivos certificados de idoneidad técnica expedidos por el Ilustre Colegio de Abogados de Lima, de conformidad con el Decreto Legislativo 681 y la Ley 26612. Correspondió en estos primeros casos de fedatarios, al Presidente de la Corte Superior de Lima, tomar el juramento o designar el Juez de Primera Instancia para que su titular sea el encargado de tomar el juramento respectivo, dejándose constancia de la diligencia, lo que permitió al Ilustre Colegio de Abogados de Lima proceder a la inscripción y registro de la firma suscrita en el archivo correspondiente, posibilitando se pueda dar inicio al ejercicio de las funciones de Fedatario Juramentado con Especialización en Informática. El Colegio de Notarios de Lima también ha otorgado certificado de idoneidad técnica a una trece notarios que asimismo son fedatarios juramentados.

El Decreto Supremo 001-2000-JUS en Marzo del 2000, con relación a los fedatarios juramentados ha precisado lo siguiente: El Diploma de idoneidad técnica para obtener el título de fedatario juramentado puede ser expedido con carácter oficial para los efectos previstos en ella, por los colegios de abogados y/o los colegios de notarios. Para estos efectos los funcionarios de los colegios antes mencionados que suscriban estos certificados o diplomas lo deben hacer previa verificación del cumplimiento de los requisitos académicos de los cursos, horas dictadas y demás requisitos legales bajo responsabilidad. Los cursos que conforman el programa de especialización y capacitación para obtener el diploma o certificado de idoneidad técnica, deberán tener un mínimo de veinte horas lectivas semanales en un periodo de dos semestres académicos, con una duración de quince semanas cada semestre. El Ministerio de Justicia supervisa la realización de estos cursos para otorgamiento del certificado de idoneidad técnica, así como los procesos de ratificación cada cinco años a partir de su otorgamiento, inscripción y acreditación mediante carnet.

Entre los cursos a dictarse en los programas de especialización y capacitación para obtener el diploma o certificado de idoneidad técnica, necesariamente deben incluirse los siguientes: Derecho Informático, Informática Jurídica aplicada a los Fedatarios , Etica Informática, Comercio Electrónico, Firma Digital, Normas Técnicas Peruanas sobre Micrograbación, Archivística Digital, Inglés Informático Jurídico, Fe Pública Informática, Seminario de investigación aplicada con sustentación de trabajo final.

Los colegios de abogados y/o notarios organizan programas de especialización y capacitación para obtener el diploma o certificado de idoneidad técnica, a cargo de profesionales expertos en la materia debidamente calificados. Para este fin están facultadas para coordinar y celebrar convenios de cooperación, sea con personas jurídicas expertas en estos conocimientos y tecnologías, sea con universidades, con escuelas de postgrado y con institutos superiores que cuenten con personal docente idóneo."

Asimismo, el Decreto Supremo 001-2000-JUS precisa el concepto de estabilidad funcional de los fedatarios juramentados al disponer en su segunda disposición final y transitoria que : *"Los fedatarios juramentados tienen es-*

tabilidad en sus funciones por cinco años hasta su ratificación, plazo en el cual, de proceder la ratificación, se emite un nuevo certificado de idoneidad técnica por otros cinco años, y así sucesivamente".

3. LA FIRMA O SIGNATURA INFORMATICA Y LA FIRMA DIGITAL

3.1. Concepto de Firma Electrónica y Firma digital

La Oficina Nacional de Procesos Electorales del Perú (ONPE), define la firma como "la combinación de trazos, puntos y espacios que realiza una persona en forma espontánea, especializada y estable, convirtiéndose en una representación gráfica convencional o distintivo propio de quien la usa como titular. Constituyendo elementos principales de la firma :la grafía capital, la caja signatural y la rúbrica. Con ellos, se determina la estructura de su trazado, se localiza los trazos dextrógiros y sinistrógiros, así como la verificación de las pasantes superiores e inferiores"[5].

"El problema de la firma, que conlleva, en muchos casos, la autenticación del documento, puede ser, sin duda, el caballo de batalla para la total aceptación a efectos probatorios de este tipo de documentos informáticos ; o, dicho de otra forma, parece como si no existiera, en la práctica diaria, otro medio de autenticación que la firma"[6]

La firma digital correspondiente a un mensaje, ya sea creado por el tenedor de un par de claves para autenticar un mensaje o por una autoridad de certificación para autenticar su certificado, debe por lo general contener un sello cronológico fiable para que el verificador pueda determinar con certeza si la firma digital fue creada durante el periodo operacional indicado en el certificado, que es una condición para poder verificar una firma digital.

3.2. La firma o signatura informatica y el sistema de microforma digital

Conforme la Ley 26612 y su reglamento el Decreto Supremo 001-2000-JUS se establece los siguiente :

a) Los datos informatizados de las entidades públicas y privadas deberán tener los sistemas de seguridad e integridad que garanticen su inalterabilidad e integridad la cual puede incluir uso de firma o signatura informática.

b) Entiéndase tanto para su uso en las entidades públicas, como en las privadas que la firma o signatura informática a que se refiere la ley, incluye la firma digital, la cual será únicamente utilizada por el depositario de la fe pública para autenticar procesos de micrograbación en la obtención de microformas con valor probatorio y efecto legal.

   Las microformas así obtenidas pueden ser utilizadas en los microarchivos, en la transferencia electrónica de fondos, en la transferencia electrónica de datos informatizados y otros servicios de valor añadido, conservando su valor probatorio y efecto legal.

c) La firma o signatura informática, incluida la firma digital deberá ser comprobable su autenticidad en forma indubitable. Tratándose de firma digital ésta será utilizada por depositario de la fe pública, la comprobación de su autenticidad se hará por medios técnicos idóneos incluyendo los telemáticos en general , la certificación digital y otros que proporcionen certeza y fiabilidad, así como garantía fidedigna de que se ha conservado la integridad de la información.

---

5 Resolución Jefatural Nº 101-97-J/ONPE. Diario Oficial "El Peruano". Separata de Normas Legales. Martes, 18 de Noviembre de 1997. Lima, Perú. Página 1544614.

6 DAVARA RODRIGUEZ, Miguel Angel : Ob. Cit. Pág.363.

4. IMPLICANCIAS DE LA MICROFORMA DIGITAL EN EL DERECHO EMPRESARIAL INFORMATICO

4.1. En el Ambito Tributario

a) Declaración Telemática de Tributos.

Mediante Resolución de Superintendencia Nº 080-99/SUNAT se aprobaron las normas para que las entidades empleadoras cumplan con presentar la declaración jurada respecto de los tributos que inciden en las remuneraciones de sus trabajadores, así como para declarar a sus trabajadores, pensionistas y derechohabientes.

Mediante Resolución de Superintendencia Nº18-2000/SUNAT publicada el 30 de Enero del 2000 se amplía el uso del Programa de Declaración Telemática (PDT) y se optimiza las funciones de registro y de liquidación de tributos, con la finalidad de facilitar el cumplimiento de las obligaciones tributarias formales y sustanciales a cargo de las empresas.

El artículo 88 del Código Tributario dispone que la Administración Tributaria puede establecer para determinados deudores la obligación de presentar la declaración tributaria por medios magnéticos, entre otros. En uso de estas facultades mediante Resolución de Superintendencia Nº 019-2000/SUNAT se establece el Programa de Declaración Telemática del Impuesto a la Renta correspondiente al ejercicio gravable de 1999 para principales contribuyentes que hayan obtenido rentas de tercera categoría.

Con el uso de la microforma digital estas declaraciones en línea, cumplidos los requisitos formales y técnicos tendrían pleno valor pobatorio y efecto legal.

b) Revisión Contable tributaria

El Decreto Legislativo 681 y el Decreto Supremo 001-2000-JUS establecen que los revisores e inspectores fiscales, superintendentes, auditores y contables, funcionarios públicos competentes, revisarán la documentación micrograbada, mediante el uso de los equipos técnicos de recuperación visual, pantallas, visores, redes interconectadas telemáticamente y artefactos similares, que les deben proporcionar las empresas y entidades públicas y privadas sujetas a supervisión, inspección o auditoría, las cuales para este fin proporcionarán tales medios técnicos y las comodidades necesarias. No se exigirán copias de papel de los documentos que tienen que ser revisados".

c) Comprobantes de Pago Electrónicos

Con el uso de la microforma digital se permite el uso del comprobante de pago electrónico, sea factura, boleta de venta u otro con pleno valor probatorio y efecto legal suceptible de ser transmitido telemáticamente, lo cual para empresas y los negocios virtuales tiene gran trascendencia.

4.2. En el Ambito Societario y del Mercado de Valores

a) Sesiones No presenciales.

La Ley General de Sociedades norma las sesiones no presenciales de las sociedades anónimas tanto de Junta de Accionistas como Sesiones de Directorio. Estas sesiones no presenciales pueden realizarse utilizando la microforma digital a través de documentos informáticos en multimedia que cumplan los requisitos técnicos y formales teniendo pleno valor probatorio y efecto legal.

b) Negociación Electrónica de acciones y valores

La Negociación Electrónica de valores con anotación en cuenta incluidas las acciones está regulada en la Ley del Mercado de Valores Peruano. La microforma dado su pleno valor probatorio y efecto legal y su transmisión te-

lemática puede ser utilizada plenamente en estas negociaciones electrónicas dándole plena seguridad y fiabilidad a estas transacciones.

c) Uso en el Sistema Previsional

Conforme la Resolución Nº 055-99-EF/SAFP las AFP pueden ser autorizadas para utilizar el sistema de microforma digital tanto para la Carpeta individual del afiliado, la planilla de pago de aportes previsionales y otros documentos.

d) En el Sistema Bancario

La mircroforma digital puede ser utilizada para la conservación de documentos de los bancos durante diez año conforme a ley, para la transferencia electrónica de fondos, para la transferencia electrónica de datos informatizados y otros servicios de valor añadido incluidos los servicios en línea en Internet.

4.3. En otros ámbitos

a) Competencia Desleal

La Ley de Competencia Desleal modificada por la Ley 26612 considera desleal la adquisición de secretos por medio de espionaje, acceso indebido a la microforma digital incluida cuando es transmitida telemáticamente.

b) Protección al Consumidor

El ejercicio de los derechos de los consumidores de información, de acceso a una variedad de productos, en sus operaciones de comercio electrónico pueden ser ejercida utilizando microforma digital con el beneficio que para cualquier procedimiento administrativo y legal estos mensajes de datos donde ejercieron sus derechos tendrán pleno valor probatorio y efecto legal.

Comercio Electrónico, Consideraciones en Torno a una Nueva Area de Trabajo en Materia Fiscal

Italo Fernández Origgi (Perú)
Especialista en Derecho Tributario. Egresado de la Facultad de Derecho y Ciencias Políticas de la Universidad de Lima.

1. INTRODUCCION

Estadísticas. A mayo de 1,999 existían alrededor de 171 millones de personas a lo largo del mundo en aptitud de conectarse a Internet, cantidad que hoy día se ha incrementado y que se incrementa a un ritmo sostenido y constante. Se estima que para el año 2,005 el 20% del total de las compras mundiales se realizará a través de Internet, proporción que continuará en alza. Recientes proyecciones de la OCDE señalan que el comercio electrónico alcanzará un valor de US$ 330 billones en el período comprendido entre los años 2,000 y 2,001 y para el período 2003 a 2005 se proyecta una cifra que bordea el trillón de dólares de los Estados Unidos de América.

Hechos. Hoy en día la importancia que ha cobrado la red (world wide web) se muestra en la existencia de un mercado de dimensiones globales al que pueden acceder tanto ofertantes como demandantes, de la más amplia gama de bienes y servicios, sin ningún límite de fronteras, el cual se encuentra en operación todos los días del año, a toda hora, y además con condiciones de competencia similares para todos los sujetos intervinientes.

Los orígenes. Hacia una explicación del fenómeno de Internet podemos remitirnos a sus inicios los cuales se fundamentan en una serie de investigaciones realizadas en los sesentas por el Departamento de Defensa de los EE.UU., los cuales posteriormente deslindaron en la generación de un protocolo o lenguaje que permite el diálogo dentro de la red de distintos sistemas informáticos, hecho que a su vez permitiría el crecimiento ilimitado de ésta "telaraña" informática. Posteriormente, en los ochentas, investigadores científicos vinculan sus computadoras formando las primeras redes, a través del correo electrónico o e-mail. Finalmente, el gran salto hacia Internet como lo conocemos, es ocasionado por la aplicación de las interfaces gráficas o hipervínculos, los cuales nos permiten ir de un lugar en la red (web site) a otro con un simple clic del ratón. Podemos afirmar que es precisamente este avance el que por fin permite el despegue y apogeo de la red.

El concepto. "Una vasta red de redes internacional que permite a computadoras de todo tipo compartir servicios y comunicarse en forma directa". Esta definición fue formulada por el Departamento del Tesoro Norteamericano dentro del informe que emitiera en noviembre del año 1,996, producto de una investigación realizada en torno a las implicancias de política fiscal derivadas del comercio electrónico internacional[1]. En relación a ésta definición debemos señalar nuestro acuerdo, en donde se advierte una flexibilidad acorde con la naturaleza de lo definido y donde se puede destacar lo que para nosotros constituye el elemento tipificante de Internet, la carencia de ubicación en un espacio físico. A propósito de dicha característica, cabe afirmar que resulta determinante a fines de establecer cualquier regulación o efectuar cualquier análisis en torno a las implicancias legales o comerciales de Internet (como veremos más adelante).

Hiperactividad ahora. Cabe preguntarse, pero que está pasando con Internet y porqué reviste tanto interés en sectores como el empresarial, financiero o gubernamental?. La respuesta es simple; Internet se puede considerar el mayor mercado, con el mayor índice de crecimiento de los últimos tiempos (sino de toda la historia). A través de Internet podemos implementar un servicio de ofrecimiento de óvulos de hermosas modelos para ser fecundados con el esperma del comprador, también podemos brindar servicios integrales de presentación y pago de facturas,

[1] Department of the Treasury, Office of Tax Policy. "Selected Tax Policy Implications of Global Electronic Commerce". Noviembre de 1996. <http:// www.jya.com/taxpolicy.htm>.

también podemos vender discos y libros, sean como bienes corporales o digitalizados, inclusive podríamos intentar prestar el servicio de acceso a Internet en forma gratuita con el objeto de obtener rentabilidad cobrando a empresas comerciales por colocar publicidad en el camino de los usuarios o, en todo caso, cobrando un porcentaje del tráfico generado para el operador de telecomunicaciones, con quien se podría formar una alianza estratégica. El comercio a través de Internet, es decir el comercio electrónico, se ha tornado en una creación hiperactiva, cuyas cifras de intercambio llaman la atención de todo el mundo.

Importancia. Dentro de los parámetros considerados en el párrafo precedente podemos afirmar que, Internet a llegado para cambiar los esquemas del comercio como los conocemos en la actualidad. En análisis publicados por empresas como AT & T, Just in Time e Intuit, cuyos negocios se encuentran seriamente comprometidos en el desarrollo de este nuevo sector, se señala que Internet cambiará la forma en que interactúan compradores y vendedores en el mercado. Así, el cambio se está formando hoy mismo.

Fiscalidad. En este contexto, llegamos a la materia que nos preocupa. Resulta evidente que, en un mercado cuyas cifras son tan significativas, no tarde en salir a relucir el interés de la administración fiscal con el objetivo de captar la recaudación respectiva. Es aquí donde empieza nuestro trabajo al analizar las implicancias derivadas de la aplicación de las cargas impositivas a Internet y el comercio que se realiza a través del mismo, además de la factibilidad de su aplicación en la práctica. En este sentido, debemos apreciar básicamente cuáles deben ser los principios y criterios atendibles al momento de establecer el régimen tributario aplicable a Internet, es decir considerando implicancias de política fiscal y de la actividad de la administración fiscal.

En consecuencia, no es objeto del presente trabajo recomendar o dejar de recomendar la aplicación de nuevas o antiguas formas impositivas a las transacciones comerciales que se realicen por Internet. Pretendemos brindar criterios sobre los cuales se pueda sopesar una decisión apropiada respecto al tema, sobre todo tomando en consideración la diversidad de factores que se presentan en realidades como la de países desarrollados y de países cuya situación es de claro atraso respecto de aquellos.

2. ASPECTOS TECNICOS

Como podemos ver, Internet facilita un medio de comercio el cual no requiere de un establecimiento físico alguno y que incluso permite la transmisión digitalizada de bienes que tradicionalmente se han transado como bienes corporales. En este tema saltan a la vista los casos de venta de música y libros en formatos digitalizados, los cuales son remitidos vía electrónica al comprador (sin necesidad de soporte físico alguno). Dentro de este nuevo esquema cabe preguntarse dónde podría intervenir un adecuado control fiscal el cual permita determinar la afectación tributaria correspondiente a dichas operaciones, sobre todo donde en apariencia el vendedor carece de presencia física o nexo que lo vincule con alguna jurisdicción.

Como señala el especialista Alvaro de Juan Ledesma[2], la doctrina internacional se encuentra dividida en dos tendencias respecto a la fiscalidad del comercio electrónico. Podemos observar una primera corriente de opinión que señala que, el comercio electrónico no genera problemas distintos en materia fiscal a los que ya han generado otros avances tecnológicos cuyo procedimiento en alguna medida guarda relación con la operatividad de Internet (p.e. ventas telefónicas). De otro lado, están aquellos que consideran que Internet supone un cambio estructural en materia de fiscalidad, dado lo cual deben ser dejados de lado los conceptos tributarios tradicionales, para pensar en nuevos esquemas y nuevas soluciones.

Sin embargo, a este punto nos interesa efectuar una revisión de los principales avances concretados por distintos órganos y entidades internacionales en torno a los principios rectores que deben ser observados al determinar el tratamiento fiscal de Internet.

---

[2] De Juan Ledesma, Alvaro. "Internet y Nuevas Tecnologías en Telecomunicaciones: Nuevos Retos de la Fiscalidad Internacional", Revista "Análisis Tributario", Números 141 y 142, Octubre y Noviembre de 1,999.

2.1 Criterios rectores de la fiscalidad del comercio electrónico

2.1.1 *Principios generales de política fiscal (General Considerations)*

El Departamento del Tesoro Norteamericano dentro del precitado trabajo "Implicancias de Política Fiscal del Comercio Electrónico Global"[3], ha establecido una serie de criterios rectores los cuales pretenden delimitar las pautas a observar al momento de analizar y determinar la afectación tributaria de las operaciones del comercio electrónico. En ese sentido, a continuación comentamos tales principios:

a) Enunciado general, observancia de principios y criterios fiscales vigentes

En virtud de éste enunciado se señala que, cualquier consideración relativa a materias de política fiscal o de administración fiscal relacionadas al comercio electrónico deben estar orientadas por los principios básicos ya existentes de política fiscal, pero sobre todo tomando en consideración las características de orden técnico y científico de la infraestructura global de la información, dentro de la cual se ubica Internet. Así tenemos que, se acudirá a nuevos principios de tributación sólo en casos extremos. En opinión de la Cámara de Comercio Internacional – ICC[4], la aplicación de las reglas fiscales existentes es el mejor medio de asegurar la consecuente aplicación del principio de neutralidad (el cual explicaremos a continuación), en razón de lo cual se respalda éste enunciado general.

Sobre la base de considerar que, el Estado moderno requiere y es parte inevitable de sus actividades, la captación de recursos internos los cuales le permitan solventar el ejercicio de las funciones que le corresponden como tal, entre las que se cuentan las inherentes a su condición como son las de administrar justicia o legislar, además de otras que por su carencia de interés para el sector privado debe cubrir como puede ser la realización de obras públicas en educación; la recaudación es la forma por excelencia que permite la captación de los referidos recursos. A su vez, donde cada Estado mantiene una determinada política a efectos de establecer las cargas impositivas que le posibilitarán la percepción de los recursos necesarios para cumplir sus funciones, debemos entender que los criterios rectores de dicha política deben presentar la mayor consistencia en orden a la situación especial de cada jurisdicción. Tales principios y criterios no deben ser variados en atención a situaciones coyunturales o en casos en que no se presente una real necesidad de modificación. En este sentido, si bien creemos que Internet implicará a futuro una serie de cambios de forma no meramente coyuntural, sino estructural en el comercio mundial, por el momento entendemos prematuro un intento de cambio radical en tanto que podríamos proyectarnos en un sentido equívoco dentro de estas nuevas materias.

En consecuencia, entendemos un tema de relevancia la gradualidad de los avances que se apliquen en la regulación tributaria del comercio electrónico y como punto de partida establecer la aplicación de los principios que se encuentran hoy en vigencia, salvo en casos extremos, como ya se ha indicado.

b) Neutralidad

El principio de neutralidad nos dice que la afectación tributaria de un determinado bien o servicio, no debe ser un factor determinante al momento en que el consumidor elija que producto ad-

---

[3] Department of the Treasury, Office of Tax Policy. "Selected Tax Policy Implications of Global Electronic Commerce", 6. Tax Policy and Administration Issues: General Considerations. Noviembre de 1996. <http:// www.jya.com/taxpolicy.htm>.

[4] International Chamber of Commerce. "Tax Issues and Ramifications of Electronic Commerce". Noviembre de 1,999. www.iccwbo.org.

quirir. Así, el tratamiento tributario para un tipo de bien determinado debe ser el mismo en todos los casos, de modo tal que no ejerza influencia en el consumidor al momento que este decida cual bien adquirir dentro de esa especie. Por ejemplo, en el mercado de autos, la afectación tributaria debe ser tal que no influencie la elección del consumidor entre una marca y otra o la adquisición a través de un canal de ventas u otro, dicha elección debe sustentarse en las prestaciones que ofrece cada tipo y marca de vehículo, pero no su afectación impositiva.

En ese sentido, el principio de neutralidad implica que el sistema tributario debe tratar en forma económicamente equivalente los ingresos generados por operaciones similares, lo que significa decir en el campo de la materia que nos ocupa que, una operación de compra venta de un bien determinado debe ser gravada en idéntica forma, desde el punto fiscal, tanto si es realizada a través de un canal de ventas tradicional como puede ser una tienda minorista, como en el caso de venta a través de Internet. De ésta forma el tema el tema fiscal no debe afectar la estructura económica de un mercado determinado, ni afectar el éxito o fracaso que éste pueda tener, los cuales se deberán generar en función a las condiciones del propio mercado.

Sobre este punto tenemos pronunciamientos encontrados en los que evidentemente los vendedores que utilizan canales físicos, como tiendas minoristas, respaldan la imposición de los mismos tributos que les son aplicados a las ventas que realizan para las ventas realizadas a Internet[5]. De otro lado, estarán quienes realizan ventas a través de Internet y respaldarán la exención de dichos tributos.

No obstante, el principio de neutralidad importa la no discriminación de operaciones comerciales según se hayan realizado a través de un medio tradicional o en Internet, de manera que no se desincentive la utilización de uno de estos medios en perjuicio del otro.

c) Impacto de los aspectos técnicos de Internet

Se señala que al momento de delimitar el tratamiento tributario de Internet se debe tener en consideración las especiales características técnicas que presenta de suerte tal que, no se introduzca regulación alguna sin haber entendido previamente el objeto de la misma. De ésta forma, la flexibilidad será un elemento clave en tanto que permita la adaptación de las normas a situaciones de extrema diversidad, dentro de una realidad sumamente cambiante como es la el comercio electrónico.

Entendemos que este es un principio de lógica, en virtud del cual antes de establecer alguna regulación debemos entender la naturaleza del objeto que se regula[6]. Ahora bien, dentro de estos aspectos técnicos inherentes a Internet cabe considerar básicamente los siguientes:

i. Ausencia de control central (descentralización)

Partiendo del hecho que Internet carece de toda ubicación física, se debe considerar que sus usuarios no tienen control centralizado de su información y que normalmente no saben que camino sigue la información que solicitan o la que publican. Así, en términos generales, para los usuarios de Internet carece de relevancia por donde pasan los datos que manejan. En tal sentido, resultaría muy difícil establecer un mecanismo centralizado de control

---

[5] A propósito, la Federación Nacional de Vendedores Minoristas de EE.UU se ha pronunciado en el sentido que las ventas a través de Internet deben ser afectadas tributariamente con similares gravámenes que las ventas realizadas en tiendas. Se señala que desgravar en alguna medida dichas operaciones sería una medida de inequidad. No obstante, se entiende que no correspondería la imposición de nuevos tributos para las operaciones de comercio electrónico.
Artículo publicado en <http://www4.zdnet.com:80/intweek/stories/news/0,4164,2424501,00.html.>

[6] Al respecto, el precitado informe del Departamento del Tesoro Norteamericano "Selected Tax Policy Implications of Global Electronic Commerce", contiene una explicación integral de los aspectos técnicos de Internet, partiendo desde su ubicación dentro de la "Super carretera de la Información o Infraestructura Global de la Información".

mediante el cual se lleve un monitoreo permanente de que información pasa a través de ciertos extremos de la red y mas aun que el mismo pretenda ser aplicado para afectar tributariamente la información transmitida.

Todo control que se pretendiera establecer a la transmisión de información por Internet o inclusive a los pagos que se efectúan a través de ésta, deben considerar que Internet es una red de información global y que el camino que pudiera haber seguido dicha información o pago podría haber atravesado un número indeterminable de jurisdicciones.

ii. *Ausencia de intermediarios*

Una de las características del comercio en Internet es que por lo general elimina la presencia de intermediarios comerciales. En este tema cabe señalar que, normalmente las administraciones fiscales buscan concentrar sus actividades de fiscalización en estos intermediarios comerciales en donde los consumidores finales son muy pequeños y se hace materialmente imposible llegar hasta ellos dado lo cual, en el comercio electrónico normalmente se perderá un punto, el del intermediario, sobre el cual se pueden concentrar controles fiscales.

iii. Falta de correspondencia entre el nombre de dominio de la computadora y la ubicación real del sujeto

En este punto se hace notar que el nombre de una dirección de Internet usualmente no nos dice la real ubicación física de las personas que están detrás de la misma, lo cual dificulta cualquier posibilidad de control en ese sentido.

iv. Carencia de registro de identificación

Introducir nuevas computadoras a Internet no implica dificultad alguna. Los requisitos de identificación que se requieren para ello no presentan una seguridad adecuada que permita acreditar consistentemente la identidad del usuario o por lo menos del punto de acceso a la red.

v. Control remoto

Cabe considerar que una de las características inherentes a Internet es permitir el control remoto de operaciones realizadas a través de páginas web ubicadas en distintas jurisdicciones, sin que queden rastros suficientes que permitan llegar hasta el control central de tales operaciones.

vi. Detección de contenidos

La detección del contenido de la información que se intercambia vía Internet no es muy sencilla, sobre todo si se considera técnicas de encriptación en virtud de las cuales los mensajes se hacen prácticamente indescifrables, excepto para el usuario que cuenta con la clave necesaria. Considerando que es complicado establecer claramente el contenido de la información que se transmite se debe tener mucho cuidado al intentar un control sobre la misma.

d) Moratoria sobre la afectación tributaria de Internet

De otra parte, cabe resaltar que como medida temporal y preventiva el gobierno norteamericano ha aprobado la Internet Tax Freedom Act – ITFA, la cual constituye una norma tributaria que concede una exención temporánea o moratoria sobre los tributos que pudieran afectar a Internet, considerando específicamente; (i) el servicio de acceso a Internet y (ii) los impuestos múltiples o que pudieran resultar discriminatorios respecto a operaciones realizadas vía Internet. Respecto del concepto de impuesto múltiple se precisa que, por el mismo debe entenderse la imposición reiterada por distintas jurisdicciones de una misma operación comercial mientras que, por impuesto discriminatorio se entiende la imposición de dichas operaciones con gravámenes distintos a los que normalmente se aplican a operaciones realizadas fuera de Internet.

Adicionalmente, mediante la citada norma se crea una comisión asesora en temas de comercio electrónico, la cual se encuentra encargada de conducir una investigación respecto de la fiscalidad internacional del comercio electrónico e Internet.

2.1.2 Criterios presentados por la Organización para la Cooperación y el Desarrollo Económicos – OCDE

En lo que se refiere a la OCDE, el tema de la tributación del comercio electrónico ha sido analizado en las reuniones sostenidas en Finlandia en noviembre de 1,997, en Ottawa en octubre de 1998 y en París en octubre de 1,999.

En estas reuniones la OCDE ha llamado la atención sobre una serie de materias diversas entre las que se cuentan las implicancias que conlleva la ausencia de presencia física, elemento típico del comercio electrónico, el rol que jugarán las administraciones fiscales en cuanto a temas de evasión y fraude tributario; asimismo, en cuanto a los impuestos indirectos, como es el Impuesto al valor agregado – IVA se señala que, los productos digitalizados deberían ser tratados como servicios y no como bienes. No obstante, no se ha logrado algún progreso notorio, habiéndose fijado los criterios que deberían regir el sistema tributario del comercio electrónico (trabajo similar al presentado por el Departamento del Tesoro Norteamericano), los cuales reseñamos a continuación:

- El sistema debe ser equitativo. Similar al principio de neutralidad, implica afectar con la misma carga fiscal a operaciones similares, sin importar si se han concertado mediante la red o fuera de ella.

- El sistema debe ser sencillo. Los costos administrativos y los de cumplimiento de las normas fiscales deben minimizarse.

- Seguridad jurídica. El sistema debe permitir a los individuos prever con certidumbre la carga fiscal que deberán soportar al efectuar sus operaciones de comercio electrónico.

- Sistema eficaz. El sistema debe permitir a la administración fiscal contar con medidas suficientes para eliminar el riesgo de evasión o fraude.

- Se debe evitar distorsiones económicas. La imposición fiscal no debe afectar las decisiones de los agentes del mercado. Así, las decisiones de éstos deben sustentarse en orden a consideraciones netamente económicas.

- Sistema flexible y dinámico. En orden a las características técnicas del comercio electrónico se debe regular un sistema que permita el desarrollo del mismo, adaptándose a su naturaleza cambiante.

- Sistema justo. La distribución de la recaudación fiscal entre los países debe ser equitativa.

Adicionalmente, entre las recomendaciones más importantes de la OCDE cabe mencionar que, en consideración al hecho que en las operaciones de comercio electrónico cada vez es mayor la intervención de entidades bancarias y financieras para canalizar los pagos respectivos, se podría asignar responsabilidad a estos agentes a efectos de recaudar impuestos.

2.1.3 Directrices presentadas por la Unión Europea en torno a la regulación del comercio electrónico – UE

En cuanto a los avances logrados por la UE cabe señalar que se han dictado una serie de directrices las cuales pretenden la adopción de un sistema tributario adecuado en materia de comercio electrónico, el cual se aplique a todos los países de la comunidad. A continuación nos referimos a las más importantes de dichas directrices:

- La no creación de nuevos tributos que graven el comercio electrónico. En aplicación del principio de no discriminación se establece que, se debe mantener la misma carga fiscal tanto para las ope-

raciones del comercio electrónico, como para las efectuadas por medios tradicionales.

- La transmisión electrónica de datos constituye una prestación de servicios gravada. Aquí se previene la venta de bienes en formato digitalizado, la cual se asimila a una prestación de servicios la cual resultará gravada con el IVA y con el impuesto a la Renta respectivos.

- Para garantizar la aplicación del principio de neutralidad el IVA deberá afectar las prestaciones que se realicen para consumo en la UE, independientemente del medio o fórmula comercial que se utilice para realizar la operación.

- Las normas que se implementen no deberán significar cargas ni costos adicionales para los operadores y consumidores en el comercio electrónico de manera tal que, se permita el desarrollo del mismo. Así, los procedimientos fiscales se deberán compatibilizar con las prácticas comerciales de este medio.

- El sistema debe ser eficaz, garantizando el correcto cumplimiento de las obligaciones tributarias surgidas de las operaciones electrónicas realizadas.

Adicionalmente, cabe señalar que si bien la UE descartó la posibilidad de implementar un "bit-tax", el cual implica un gravamen a las transmisiones efectuadas por Internet, midiendo para ello el número de bits transferidos; recientemente la Comisión Europea ha anunciado la implementación de un impuesto sobre la venta de mercancías virtuales respecto del cual no se han aclarado sus características.

Al respecto, consideramos que dicha decisión atenta contra el principio de no crear nuevos gravámenes que resulten discriminatorios de las operaciones del comercio electrónico. Sin embargo dicha regla puede ser inaplicada en situaciones extremas. En ese sentido, la justificación al gravamen cuya imposición se pretende podría quedar fundamentada en el hecho que tales transmisiones digitalizadas están produciendo un perjuicio serio en la recaudación, es decir que se trataría de un caso extremo que amerita la aplicación de un nuevo gravamen. Desconocemos los criterios técnicos que sustentarían la creación de dicho tributo, pues al término del presente trabajo la Comisión Europea no ha publicado ni la norma, ni el análisis correspondiente.

2.2 Nexo o vínculo tributario – establecimiento permanente

El siguiente tema el cual debemos desarrollar es el del nexo o vínculo a efectos de sujetar a un determinado sujeto a las cargas impositivas de una determinada jurisdicción. Como sabemos, normalmente los países obligan a tributar a las entidades o personas extranjeras respecto de las operaciones y por tanto, de los ingresos, obtenidos dentro de su jurisdicción, en tanto tales sujetos desarrollen actividades comerciales en forma efectiva dentro de dicha jurisdicción.

El problema dentro del comercio electrónico será definir los criterios que nos permitan determinar en que casos se considera que se desarrollan actividades comerciales dentro de una determinada jurisdicción, y en ese sentido cuando considerar que el desarrollo de actividades comerciales a través de Internet implica la presencia de un establecimiento permanente en una determinada jurisdicción.

Para la OCDE el establecimiento permanente importa un lugar fijo de negocios mediante el cual una empresa realiza todo o parte de su actividad. Así tenemos que, dentro de ésta definición se requiere la presencia de dos elementos para que se configure un establecimiento permanente, un primero (i) el elemento físico, consistente en el lugar fijo de actividades y un segundo (ii), el elemento de contenido económico, el que requiere la realización de actividades económicas. Sólo con la concurrencia de ambos elementos podemos hablar de la existencia de un establecimiento permanente.

De otra parte, cabe considerar que para el Departamento del Tesoro Norteamericano la dificultad de la determinación de la existencia de un establecimiento permanente en EE.UU. no radica en establecer si se realizan

actividades comerciales o no, sino meramente en establecer si existe suficiente presencia física en dicha jurisdicción, como para vincular al sujeto y someterlo a las disposiciones de su sistema fiscal. En ese sentido se señala que, normalmente un operador de comercio electrónico no tendrá un establecimiento permanente en EE.UU., debido a que por lo general no mantendrá un lugar físico de negocios dentro de dicha jurisdicción. En estas condiciones sólo se podrá entender la existencia de un establecimiento permanente si el mismo es creado por alguna forma de imputación.

A propósito de la imputación de dicho vínculo, consideramos de relevancia analizar la posibilidad de atribuir a una página web instalada en un servidor de una determinada jurisdicción, la calidad de establecimiento permanente dentro de dicha jurisdicción.

2.2.1 Pronunciamientos jurisprudenciales

En este tema es de notable importancia referirnos a la sentencia de la Corte Federal alemana del 30 de octubre de 1996, dentro de la cual dicho órgano se pronuncia en el sentido de considerar un oleoducto holandés, el cual cruza territorio alemán, operado mediante sistemas informáticos en forma remota desde fuera de Alemania, como un establecimiento permanente en Alemania a efectos de los impuestos sobre el Patrimonio Neto Empresarial y a efectos del Convenio sobre Doble Imposición suscrito entre Holanda y Alemania. Cabe agregar que, las instalaciones de la empresa holandesa no requerían y no utilizaban personal alguno de dicha empresa y en los caos en que se requería algún servicio de mantenimiento, estos eran subcontratados con alguna empresa alemana.

La gravedad del criterio que encierra el pronunciamiento del tribunal alemán es notoria. En este caso se está entendiendo que basta la presencia física en una determinada jurisdicción a través de maquinarias automatizadas y sin la necesidad de personal alguno, para que se entienda que existe un establecimiento permanente, el cual será suceptible de ser incidido tributariamente en la jurisdicción donde se ubiquen dichas instalaciones. Al respecto, cuestionamos el señalado criterio en orden a considerar si de acuerdo a la realidad de los hechos se podría entender que es suficiente la instalación de maquinaria automatizada para la existencia de un establecimiento permanente. Entendemos que no podrá haber establecimiento permanente donde haya ausencia de personal y de una mínima presencia organizacional.

Afortunadamente, existen pronunciamientos jurisprudenciales en sentido contrario respecto del antes señalado, entre los cuales podemos citar la sentencia del Tribunal de Justicia de las Comunidades Europeas del 17 de mayo de 1977 la cual prescribe que, no existirá establecimiento permanente, en tanto no exista la presencia permanente de medios humanos y técnicos necesarios para la prestación de servicios (debe entenderse en sentido lato, la realización de operaciones en general) y, si dicha prestación no se encuentra suficientemente vinculada con el lugar de la actividad económica del prestatario.

Entendemos, carente de sentido la posibilidad de entender una página web instalada en un servidor como un establecimiento permanente a efectos tributarios, porque debe quedar en claro que, el servidor es un medio el cual permite la comunicación del sitio web con otros sitios de Internet, no se le puede considerar como un lugar físico donde ya hemos señalado que uno de los elementos característicos desde el punto de vista técnico de Internet es que carece de toda ubicación física. Debe quedar claro que la red carece de relevancia como entidad corporal, ésta no debe ser entendida como una maraña de cables, computadoras e instalaciones similares, sino como una entidad dinámica que permite el intercambio de información entre sus usuarios. Aun mas, como bien señalan los análisis realizados por el Departamento del Tesoro Norteamericano, si se estima que la ubicación dentro de un servidor instalado en una determinada jurisdicción podría dar lugar a entender que se configura un establecimiento permanente, el incidido con dicha determinación puede fácilmente variar su ubicación para trasladarse a un servidor instalado en una jurisdicción distinta y que además podría constituir un paraíso fiscal. En suma, la ubicación de la página web del sujeto dentro de uno u otro servidor debe ser descartada como criterio de imputación a fines de establecer un establecimiento permanente.

2.2.2 Opinión de la Cámara de Comercio International

En cuanto a ésta materia coincidimos con la opinión de la CCI[7] en el sentido que, Internet crea la posibilidad de las empresas de abrir las puertas de sus negocios a una cantidad indeterminada de países (jurisdicciones tributarias), respecto de los cuales no se generará un establecimiento permanente. Así, la generación de establecimientos permanentes por dichos ofertantes estará directamente relacionada con su interés por penetrar un determinado mercado ubicándose físicamente en el mismo y dando soporte y servicios locales en distintas jurisdicciones, es decir la generación de dichos establecimientos permanentes estará determinada por las condiciones del mercado, según las características del mismo, dependiendo si se trata de la prestación de algún servicio especializado o, la venta de un bien que requiere un mantenimiento periódico, etc.

2.3 Aplicación de tributos vigentes al comercio electrónico - análisis y problemática

En este acápite nos ocuparemos de ver como se adaptan los sistemas tributarios vigentes a las operaciones de comercio electrónico, tratando básicamente los impuestos a la renta y al valor agregado, por ser los de mayor incidencia en cuanto al comercio en la actualidad.

2.3.1 Imposición a la Renta

Actualmente en la mayoría de países, en orden a establecer la afectación tributaria sobre las rentas de individuos y empresas, se grava a los residentes en función a sus rentas globales mientras que, a los no residentes o no domiciliados se les incide por sus rentas de fuente local, es decir; en el primer caso se aplica el criterio de residencia mientras que, en el segundo se aplica el criterio de la fuente. Internet otorga la posibilidad a los no domiciliados de realizar una serie de transacciones sin vincularse con ninguna de las jurisdicciones donde dichas operaciones se concretan. Ello implica que el país receptor se puede ver afectado con la pérdida de la recaudación por el Impuesto a la Renta de los no domiciliados siendo que, ésta situación podría generar una evolución hacia el criterio de la afectación tributaria sobre la base de la residencia.

Surge así un conflicto de intereses donde se contraponen las posiciones de los países exportadores (de tecnología por excelencia) y los receptores. Así, si los países receptores pierden la posibilidad de afectar tributariamente las rentas de fuente local de las empresas no domiciliadas, se debe entender la generación de una baja en la recaudación de dichos estados, lo cual deja ver ciertas dificultades de orden económico para dichos países puesto que, estos son normalmente los menos desarrollados y con necesidades urgentes de mejorar la recaudación para satisfacer las necesidades de carácter público.

No obstante lo anterior, también debemos considerar que más allá de la aplicación de formas impositivas tradicionales, es necesario establecer un sistema que permita una recaudación de forma eficaz y segura, prescindiendo de complicaciones, las cuales muy probablemente pudieran mermar la rentabilidad de recaudar el Impuesto a la Renta aplicando el criterio de la fuente para los no domiciliados. En este orden de ideas, debemos señalar que ésta materia debe ser analizada cuidadosamente y sólo en atención a un sistema fiscal que permita en forma segura, eficaz y rentable, aplicar la recaudación en la fuente para las rentas de no domiciliados generadas en el contexto del comercio electrónico. Con ello no sugerimos se abandone de plano el sistema actual, sin embargo, como resulta evidente, estos sistemas tributarios deberán ir adaptándose al comercio electrónico en forma progresiva, dado lo cual estas materias deberán ser debidamente consideradas.

En cuanto a los tratados para evitar la doble tributación debemos señalar que, actualmente su función debe significar que los individuos respecto de los cuales se verifican las obligaciones tributarias, se vean incididos y tri-

---

[7] A propósito de dichas materias, se debe señalar que ésta Institución realiza permanentes investigaciones, dentro de las cuales se ha llegado a la conclusión que, al margen de consideraciones tributarias, el sector empresarial continuará utilizando establecimientos permanentes en los países donde lo entienda necesario para el cuidado de sus clientes y por tanto de su imagen y resultados empresariales.

buten exclusivamente en el país de residencia. En tal sentido, dicha finalidad podría mantenerse vigente respecto del comercio electrónico, introduciendo los ajustes que resulten pertinentes.

2.3.2 Impuesto al Valor Agregado

En cuanto al Impuesto al Valor Agregado – IVA cabe señalar que, su aplicación responde básicamente a dos supuestos, la venta de bienes muebles, sea interna (dentro de una jurisdicción determinada) o en forma de importación y, la prestación de servicios.

a) Venta de bienes corporales

i. Operaciones internas

En cuanto a las operaciones de venta interna de bienes corporales entendemos que no cabe mayor discusión respecto al hecho que, todas las ventas de bienes muebles que se realicen dentro de una determinada jurisdicción deben recibir un tratamiento tributario idéntico en orden a la aplicación del principio de neutralidad. Así, si por ejemplo, se decidiera exonerar la venta de bienes a través de Internet en un determinado país, ello conllevaría a que todos los compradores (que cuenten con este medio) opten por realizar sus operaciones mediante la red, ahorrando la carga económica del IVA.

Una decisión como la señalada rompe claramente la neutralidad y equidad del sistema tributario, dentro del cual se podría esperar la desaparición de las operaciones bajo formas tradicionales.

ii. Importaciones y exportaciones

En cuanto a las operaciones internacionales de compraventa de bienes corporales a través de Internet cabe considerar que, el IVA respectivo será aplicado en las aduanas del país de destino de dichos bienes, y por lo tanto no debe presentarse mayor dificultad en torno al régimen tributario de estas operaciones.

b) Bienes incorporales y prestación de servicios

Diversos tipos de bienes pueden ser digitalizados y transferidos vías electrónica a través de Internet, incluyendo software, libros, música, imágenes, entre otros.

Ahora dentro de este contexto cabe preguntarse como controlar la transmisión digitalizada de un libro o de un disco compacto, sea que ésta se realice dentro de un país determinado o que se trate de una operación internacional. En este caso no se cuenta con algún elemento físico que pueda en alguna medida permitir "seguir el rastro" de la operación realizada.

Si bien desde el punto de vista tributario todo contribuyente se ve impelido a cumplir una serie de obligaciones de índole formal las cuales permiten a la administración verificar el debido cumplimiento de sus obligaciones tributarias sustanciales, en el presente caso, el contribuyente muy bien podría omitir tales obligaciones y esperar no ser detectado. No obstante, entendemos que el comercio electrónico no será tomado como un medio para concretar nuevos casos de evasión tributaria, sobre todo donde tenemos empresas de gran envergadura las cuales gozan de un prestigio ya ganado y de una posición importante en el mercado, situación ante la cual el intento de evasión tributaria recurriendo al incumplimiento de obligaciones tales como emitir la facturación correspondiente a las operaciones realizadas o, no realizar los registros contables respectivos, podrían resultar más perjudiciales que cumplir con tributar de acuerdo a la normatividad vigente.

De otra parte, en cuanto al tema técnico cabe señalar que, respecto a la transferencia de bienes digitalizados se pueden considerar varias alternativas. Dentro de estas alternativas se cuenta la posibilidad de que lo que se

transfiera por el formato digitalizado sea un bien material en si mismo, como un libro, o que se otorgue el derecho para el uso de dicho bien incorporal. En ambos casos entendemos que el IVA debe precipitarse sobre ambos tipos de operaciones.

No obstante, entender la operación de una u otra forma presenta distinta incidencia respecto de la imposición a la renta, dentro de la cual se entiende que la transferencia de un bien corporal desde el exterior por un sujeto no domiciliado no genera renta de fuente local. Distinto es el caso de la cesión de derechos de uso sobre la propiedad inmaterial, donde se supone que el pago otorgado en retribución constituye una regalía, la cual si se entiende como una renta de fuente local y por tanto en la mayoría de países se sujetará a una retención por el pagador de la renta[8].

Hacia una solución de este problema podemos plantear el atender la naturaleza misma del bien que se está transfiriendo, es decir, si lo que se otorga es el derecho de uso de un programa informático, resultará evidente que estaremos en el caso del pago de una regalía sujeta a las retenciones que señalen las disposiciones pertinentes; empero, en el caso del formato digitalizado de un libro, sea cual sea la forma que adopten las partes, el objeto de la transferencia es un bien corporal, en razón a lo cual se debiera establecer el régimen tributario aplicable.

Si bien aun no se dispone de criterios claros ni de normas que establezcan que hacer ante estas nuevas implicancias del comercio electrónico, entendemos que el criterio que se debería utilizar para resolver situaciones complejas tales como la reseñada en los párrafos precedentes, sería la de analizar las operaciones por su verdadero contenido económico y atender a la verdadera intención de las partes. En otras palabras, si bien la tecnología puede hacer más compleja la labor al determinar la afectación tributaria de una operación, no se debe perder de vista el verdadero contenido económico de la misma con la finalidad de calificarla y por ende establecer la carga impositiva que realmente corresponde.

Finalmente, es conocida la posición que señala que este tipo de complejidades pueden ser resultas considerando que la transferencia de bienes digitalizados importa una prestación de servicios. Al respecto debemos precisar que, dicho tratamiento podría llevar a una serie de inequidades en donde se le otorgaría a ciertas operaciones el tratamiento tributario diseñado para otras, lo cual carecería de toda consistencia.

2.4 Rol de la Administración Fiscal

La intervención de la Administración Fiscal dentro del comercio electrónico debe incidir en el desarrollo del mismo. Sin embargo, dicha intervención debe ser tal que permita asegurar la captación de los recursos fiscales que correspondan de acuerdo a Ley.

Ahora, el enfoque que debe advertir toda administración respecto del desarrollo de los negocios en Internet, importa la bifurcación de este medio en dos tendencias de negocio; una primera, (i) relación empresa - consumidor final y una segunda, (ii) relación empresa - empresa. Es respecto de ésta última tendencia que se debe poner especial incidencia pues es la que presenta un mayor índice de crecimiento y un mayor volumen económico.

De otra parte, la administración deberá intervenir utilizando métodos apropiados dentro del comercio electrónico. Así por ejemplo, en el supuesto que a nivel empresarial constituye un requisito tributario la sustentación documentaria de gastos y en general para el ejercicio de derechos fiscales, es consabido que las empresas requieren de comprobantes emitidos por sus proveedores con los cuales puedan acreditar el haber incurrido en tales gastos. Dentro de este campo puede ser de gran ayuda la regulación de la facturación telemática, respecto de la cual cabe señalar que existen países que la vienen aplicando con éxito.

---

[8] Sobre este punto cabe considerar adicionalmente las complicaciones que se presentan respecto de medios de pago electrónicos los cuales no permiten practicar retención alguna. Ante ésta situación la alternativa es aplicar el concepto de gross-up, el cual importa cancelar el monto del impuesto en forma adicional. Sin embargo, esto supone un sobre costo excesivo aun más, donde el importe pagado en forma adicional no sería aceptado como gasto para el pagador de la renta.

Igualmente, puede ser de invaluable ayuda la información de terceros normalmente intermediarios en el comercio electrónico, tales como operadores del sector telecomunicaciones o del sistema financiero, quienes podrían facilitar en cierta medida la actuación de verificaciones tributarias.

3. ASPECTOS ECONOMICOS

En cuanto al tema económico y la tributación del comercio electrónico se presentan una serie de implicancias de suma importancia las cuales pasamos a tratar.

3.1 Crecimiento económico

Somos testigos del enorme crecimiento que ha experimentado el comercio electrónico en un pequeño período de tiempo, que es el que lleva de existencia. Esta nueva modalidad de comercio importa la generación de un nuevo valor agregado para la economía mundial, incluyendo nuevas modalidades de operación que agilizan y hacen más rentable el comercio, sin contar con que Internet es un sector que está generando considerables fuentes de empleo.

En ese sentido, resulta conveniente para todos el crecimiento sano de esta nueva modalidad de comercio. Sin embargo, si se afectan las operaciones realizadas en Internet con nuevos tributos en violación del principio de neutralidad, o aplicando cargas impositivas discriminatorias, el efecto directo de dichas medidas será el incremento de los precios y por lo tanto la contracción de la demanda dentro de este mercado. El efecto indirecto de este tipo de medidas resulta aun más grave dado que importa perjudicar el desarrollo del comercio electrónico, lo cual finalmente genera una merma en el desarrollo futuro de la economía en general.

En consecuencia, la recomendación en este sentido se hace evidente; antes de determinar la incidencia fiscal que debe aplicarse sobre las operaciones realizadas en el ámbito del comercio electrónico, deberá estimarse y evaluarse el efecto que puede tener dicha inserción fiscal en el crecimiento del sector y por ende en la economía global.

3.2 Neutralidad

Si se decidiera gravar las operaciones del comercio electrónico con tributos discriminatorios, como hemos visto en el acápite precedente, se estaría claramente favoreciendo el sector de operaciones tradicionales, es decir las ventas en tienda.

A este respecto se debe precisar que, la mejor forma de obtener neutralidad en cuanto al tema fiscal es, por el momento, imponer similares gravámenes tanto para las operaciones realizadas en formas tradicionales como para las realizadas a través de Internet. Muy probablemente ésta no sea la mejor fórmula pero actualmente no disponemos de otra. Quizás este sea el momento de rediseñar sistemas fiscales y redistribuir los puntos de tributación de modo tal que, la recaudación provenga de medios más apropiados, sin afectar la neutralidad y la necesidad de crecimiento económico.

Específicamente sobre el IVA cabe señalar que, los impuestos indirectos no son la forma ideal en cual el estado se puede permitir una inserción fiscal en la economía individual de los contribuyentes. No obstante, hoy en día dichos impuestos indirectos son una considerable fuente de ingresos para las economías de casi todo el planeta y más aun, para las economías de los países menos desarrollados, en los cuales el fuerte del ingreso fiscal se percibe de tributos como el IVA.

3.3 Importancia de la recaudación tributaria

Como hemos señalado, el estado moderno tiene una serie de obligaciones y funciones que cumplir y para ello requiere de la captación de recursos económicos. El medio por excelencia que le permitirá la captación de ta-

les recursos es la tributación. Sin embargo, ésta recaudación debe ser obtenida en base a un sistema tributario sano y justo, el cual permita la inserción fiscal del estado, pero sin perjudicar el desarrollo de la economía.

Ahora bien, cuando hablamos de que el estado moderno debe recaudar para cumplir con sus funciones por un lado, y por el otro decimos que, la carga fiscal no debe impedir el desarrollo de la economía, no estamos hablando de intereses encontrados. Por el contrario, un sistema tributario económicamente neutro y desarrollado sobre fundamentos de equidad, permite tanto al estado cumplir con sus fines, como al sector comercial desarrollar sus actividades en beneficio de la economía en general.

No obstante, a este punto debemos distinguir entre los lineamientos que se observan al distribuir la carga fiscal en países desarrollados a diferencia de los países con retraso económico, como son los países latinoamericanos. Mientras que los primeros centran la mayor parte de su ingreso fiscal a través de impuestos directos, más precisamente el impuesto a la renta, los segundos se ven en la obligación de apelar a los impuestos indirectos. Estos impuestos indirectos inciden a los contribuyente sin tomar en consideración sus condiciones personales, es decir afectan a todos los individuos de igual forma sin importar su real situación económica. En consecuencia, cuando hablamos de un sistema cuya recaudación proviene en su mayor parte de tributos indirectos, podemos entender que, en principio, y al menos teóricamente, no se trata de un sistema óptimo, pues no atiende la real capacidad de contribución de cada individuo.

Como hemos señalado, Internet nos pone hoy en día ante nuevos retos en cuanto a política fiscal y si bien consideramos que aun no es el momento de concretar cambios radicales mediante reformas legislativas, también consideramos que es el momento adecuado para analizar los fundamentos de los sistemas fiscales vigentes con la intención de mejorarlos en un futuro cercano.

Asimismo, en la actualidad se habla mucho sobre la posibilidad de desgravar las operaciones realizadas en Internet, sobre todo de tributos indirectos como el IVA de modo tal que, se favorezca el crecimiento del sector. Sobre estas propuestas debemos señalar que, al margen de atentar contra el principio de neutralidad y pasar a influenciar indebidamente las decisiones de los agentes del mercado al momento de hacer negocios, se debe tener presente la incidencia que representaría económicamente para países que sustentan sus sistemas fiscales en tributos indirectos.

A este propósito cabe destacar la importancia que ha presentado el hecho de mejorar la recaudación tributaria a fines del saneamiento de economías como las latinoamericanas, entre las cuales el caso del Perú resulta un ejemplo claro de mejoramiento en base a una serie de medidas entre las que se cuenta el fomento del ahorro público mediante una mayor recaudación tributaria y el control del gasto público. En estos casos la pérdida o reducción de ingresos fiscales representaría un grave perjuicio económico para las economías locales.

4. CONCLUSIONES

1) Si bien el comercio electrónico implica un cambio estructural en cuanto a la manera en que los agentes del mercado se relacionarán al momento de hacer negocios, actualmente no es el momento oportuno de crear nuevas formas legislativas para regularlo, sino que se deberán aplicar las formas y principios tributarios vigentes, salvo en el caso de situaciones extremas en las que sea indispensable la aplicación de medidas excepcionales, con el objeto de corregir alguna distorsión económica o alguna desviación en el comportamiento de empresas o consumidores (evitar evasión o fraude).

2) La aplicación del principio de neutralidad resulta de primera prioridad tanto desde el punto de vista jurídico - tributario como económico puesto que, en virtud de dicho principio se mantiene la equidad en cuanto al tratamiento fiscal del mercado en general, permitiendo que este se desarrolle o, en su caso, determinada oferta o sector desaparezca, pero en base a las propiedades inherentes a las condiciones del mercado mismo (y no por la incidencia generada de una política fiscal inadecuada).

3) Internet es un medio el cual carece de ubicación en un lugar físico, en razón de lo cual al momento de establecer el tratamiento tributario a otorgarse a las operaciones a realizarse a través del mismo se deberá atender a dicha circunstancia, prescindiendo de criterios de atribución de ubicación física en función de instalaciones puramente informáticas para los operadores de este tipo de comercio.

4) A efectos de establecer el tratamiento tributario que deberá aplicarse a las transmisiones digitalizadas, se deberá atender al objeto que constituye materia de la transacción, es decir calificar tales operaciones en función de su contenido económico de suerte tal que, se determine si en el fondo se trata de la venta de un bien corporal, el cual ha sido digitalizado para ser transado en Internet o, en su caso, la cesión en uso propiamente dicha de un bien inmaterial. En base a éstas previsiones se otorgará un tratamiento fiscal a cada operación en armonía con su propia naturaleza y objeto.

5) Las Administraciones Fiscales deben intervenir en el comercio electrónico propulsando su desarrollo, a la vez que asegurando la percepción de la recaudación que establece cada sistema. Para ello deben aplicar las facilidades que permite la tecnología pero, considerando las características inherentes a Internet en razón de lo cual deberán aplicar criterios flexibles en el cumplimiento de sus funciones.

6) Antes de determinar las cargas impositivas que deben fijarse para el comercio electrónico deben analizarse las implicancias que dichas cargas traerán respecto del desarrollo del sector y por tanto de la economía en general. En la medida de lo posible se deberán favorecer los avances en materia de técnica fiscal, con el objeto de lograr la aplicación de un sistema que permita al Estado recaudar los fondos suficientes para cumplir sus funciones, a la vez que se permita el desarrollo de las economías locales y global.

7) Al momento de analizar las incidencias económicas de la fiscalidad de Internet al interior del mercado, también se deberá tomar en consideración la incidencia que podría representar la adopción de medidas tales como desgravar ciertas operaciones de tributos indirectos, sobre todo en el caso de economías débiles, las cuales dependen en mucho de los tributos indirectos para lograr las metas necesarias de recaudación fiscal. Esto considerando el contraste existente respecto de economías fuertes, las cuales ocasionan el grueso de dichas entradas en la tributación directa.

BIBLIOGRAFIA

1) Atkinson, Robert y Court, Randolph. "Internet Taxation, a Software Solution". Setiembre de 1,999. <http:// www.ecommercecommission.org/library.htm>.

2) Blackhurst, Paul. "Adam Smith and E-commerce?". Febrero 2,000. <http:// www.mce.be/article/ecom.htm>.

3) Department of the Treasury, Office of Tax Policy. "Selected Tax Policy Implications of Global Electronic Commerce". Noviembre de 1996. <http:// www.jya.com/taxpolicy.htm>.

4) De Juan Ledesma, Alvaro. "Internet y Nuevas Tecnologías en Telecomunicaciones: Nuevos Retos de la Fiscalidad Internacional", Revista "Análisis Tributario", Números 141 y 142, Octubre y Noviembre de 1,999.

5) Del Moral, José A. "Los impuestos del Ciberespacio". Revista Electrónica de Derecho Informático - REDI. Junio 1,999. <http://publicaciones.derecho.org/redi/N@umero_11_-_Junio_de_1999/moral>

6) Gildemeister Ruiz-Huidrobo, Alfredo. "Derecho Tributario Internacional: Los Establecimientos Permanentes". Fondo Editorial 1,995 Pontificia Universidad Católica del Perú. Lima, 1995.

7) International Chamber of Commerce. "Tax Issues and Ramifications of Electronic Commerce". Noviembre de 1,999. www.iccwbo.org.

8) Owens, Jeffrey. "Electronic Commerce, Answering the Emerging Taxation Challenges". Novienbre 1,999.
<http:// www.ecommercecommission.org/library.htm>.

9) R. Bruce Josten. "E-commerce Taxation: Issues in Search of Answers". Setiembre 1,999.<http:// www.ecommercecommission.org/library.htm>.

10) Revista Tributaria. "E-commerce". Junio 1,999. Número 6.

Internet en el contexto del Comercio Internacional y las Pautas de Tributación en el Impuesto a las Ganancias Argentino

Juan P. McEwan[1] (Argentina)

Este primer trabajo tiene por finalidad efectuar un análisis de este "nuevo" canal de comercialización llamado Internet. Partiendo del entendimiento de las características propias y funcionamiento de "la red", se finalizará efectuando una aproximación de los distintos elementos a tener en consideración ante una eventual delimitación de la imposición sobre la renta a los negocios operados por intermedio de esta vía de comunicación.

1. INTRODUCCION

El avance tecnológico constante que se ha experimentado en el siglo XX ha creado ciertamente infinidades de desafíos no solo en el campo del derecho en general sino también en el campo de la tributación. La velocidad y avance que han tenido las comunicaciones a nivel mundial han originado nuevas formas de comercialización de productos, resultando en definitiva un acercamiento de los países del mundo y una conexidad económica impensada décadas atrás. Gracias a estos fenómenos hoy estamos envueltos en la llamada globalización económica mundial.

Por medio de Internet se ha creado un nuevo desafío para juristas, gobernantes, jueces, empresarios, inversionistas, etc. Este nuevo reto implica la regulación legal necesaria para la protección y defensa tanto de las derechos individuales de las personas como de los derechos colectivos necesarios para la vida en comunidad, como ser el derecho tributario.

El crecimiento vertiginoso que ha experimentado Internet desde su creación (1969) al presente, no solo en el orden de usuarios sino también en la cantidad de operaciones comerciales efectuadas a través de ella, ha puesto en alerta a los gobernantes de las grandes economías del mundo en busca de soluciones en el campo legal general pero más aún en el campo de la tributación internacional, en vista de las particularidades que envuelve esta vía de comercialización cibernética.

Como ejemplo podemos citar al Departamento del Tesoro de los Estados Unidos (United States Treasury Department), que ha puesto a las transacciones efectuadas por medio de Internet como "primera prioridad" internacional. De acuerdo con Carol Doran Klein, responsable de Consultoría Internacional Tributaria del Departamento de Política Tributaria de ese país, "*Las posibilidades de Internet recién comienzan a ser exploradas, como ser las implicancias impositivas de hacer negocios en Internet*"[2]

Esto promueve el estudio de nuevas fronteras en la práctica de imposición, la naturaleza de los propios negocios electrónicos nos lleva a evaluar su composición para comprender el funcionamiento de esta inédita herramienta de comercialización. Por ser Internet un nuevo fenómeno en el cual los especialistas en tributación no podrán evitar verse involucrados en un próximo futuro, es necesario comenzar con el "ABC" de la cuestión, es decir, el funcionamiento básico de esta ruta de comercialización.

2. EL ORIGEN DE LA HOY LLAMADA RED DE REDES: INTERNET

Internet remonta sus orígenes a la "guerra fría". En los años '60 los Estados Unidos de Norte América y la ex-Unión Soviética se encontraban en plena expansión armamentística y a las puertas de una nueva guerra mundial

---

[1] Abogado. Especialista en Derecho Tributario. Miembro integrante del Area de E-Commerce del Estudio PricewaterhouseCoopers. Buenos Aires, Argentina.

[2] "International Taxes: Financial Services, Internet, Among Top Foreign Issues, Treasury Department Official Says", Daily Tax Report, (Taxation, Budgett and Accounting, January 19, 1996), The Bureau of National Affairs.

(y quizá la ultima). En vista a ello, el gobierno de los Estados Unidos tuvo que enfrentar un problema de milicia estratégica: ¿cómo las autoridades americanas podrían comunicarse frente a un ataque atómico por parte de su "rival"?.

Estados Unidos comenzó a experimentar nuevas formas de comunicación, donde la base de información no se encontrare ubicada exclusivamente en un determinado lugar, así bajo la Agencia del Pentágono encargada de los proyectos de estudios avanzados (Advanced Research Project Agency) también conocida como -ARPA-, se formó la red de comunicación mas avanzada del mundo, siendo bautizada con el nombre de "Arpanet".

Los principios elementales seguidos para la creación de esta nueva red eran que todos los "nodos" (puntos de conexión) debían ser igual en status, cada uno podía enviar y recibir mensajes; que todos los mensajes debían ser mandados en "packets" (ensobrados), cada uno con su propia dirección y que cada packet debía ser enviado por un usuario, debiendo ser recibido bajo la dirección de otro usuario (esto significaba que si un usuario era eliminado, podrían los restante usuarios continuar comunicándose a través de la red). Hoy en día Internet aplica similares metodologías en el envío de información.

Arpanet en un principio se encontraba bajo la propiedad de la milicia, siendo utilizado exclusivamente por aquellos contratistas del estado y universidades que conducían trabajos o investigaciones relacionadas con la defensa del país. Posteriormente, el gobierno autorizó a tener acceso directo, por intermedio de laboratorios y universidades, a investigadores de todo los Estados Unidos. En la década de los '90 se generalizó el uso, modificándose el nombre por "Darpa Internet" y, finalmente, llegándose al nombre con que hoy se conoce, "Internet".

3. ¿QUE ES INTERNET?[3]

Desde sus comienzos se intentó crear un sistema de comunicación descentralizado, es decir, que cada centro emisor y recibidor de información (link) no tenga relación directa con el otro (si uno dejase de funcionar no perjudicaría a los demás links), pudiéndose transmitir información sin la intervención o control humano directo y con la capacidad de redireccionar automáticamente la transmisión si uno o varios links fueren dañados.

El Estado creador de este innovador medio de comunicación, por medio de una Resolución de fecha 24 de agosto de 1995 del Consulado Federal de Redes (Federal Networking Council –FNC-) ha definido Internet como *"El sistema global de información que (a) se encuentra lógicamente inter-conectado por direcciones únicas globales basadas en el Protocolo Internet (IP) o sus consecuentes extensiones; (b) es posible soportar comunicaciones haciendo uso del Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP[4]) o sus consecuentes extensiones, y/u otro IP –compatibles protocolos-; y (c) provee o hace accesible, públicamente y privadamente, alto nivel de servicio basado en las comunicaciones e infraestructuras descriptas."* [5]

---

[3] "Internet es mayormente software. Nosotros hablamos sobre ella como si fuera hardware, computadoras personales, routers y fibra óptica, pero el corazón de Internet es el software utilizados como aplicaciones y protocolos. Software es infinitamente maleable y cualquiera que pueda desarrollar un programa puede hacerlo (...). Yo anticipé grandes sorpresas y cambios monumentales en la forma en que la Red pueda servirnos, simplemente basado en el hecho de que Internet es software, y el software puede hacer cualquier cosa" –Vicent Cerf, Senior Vice President, MCI & One of the Fathers of the Internet-.

[4] Como su nombre implica, un protocolo es una lengua común que se establece en dos para que éstas puedan comunicarse. Existen infinidades de protocolos. En Internet, el protocolo más importante es el IP o TCP.

[5] FNC RESOLUTION: Definition of "Internet". "The Federal Networking Council (FNC) agrees that the folowing language reflects our definition of the term "Internet".

"Internet" refers to the global information system that –

a) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;

b) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP –compatible protocols; and

c) provides, uses or makes accesibles, either publicly or privately, high level service layered on the communications and related infrastructure described herein."

Traduciéndose a palabras simples, es un grupo de computadoras denominadas servidores (servers), conectadas entre si -similar al sistema telefónico internacional, es decir, interligados por cables ópticos, líneas conmutadas[6] y otras, dependiendo de la conexión y ubicación mundial-. Estos servidores tienen la característica particular de almacenar infinidad de información, separada por archivos o mejor conocidos como "páginas" (sites) desde una computadora personal, al establecer contacto, se puede consultar.

Cada transmisión efectuada a través de la red es simplemente un intercambio de información, este intercambio de datos o información electrónica no difiere en gran medida con el servicio de correo que todos conocemos; cada uno tiene una dirección y para enviar o recibir información no se necesita más que la dirección (IP numbers/Internet Domain Name) para encontrar o dirigirse al destino deseado; ya que Internet esta provista de infinidades de servers conectados, formándose distintas rutas y conforme la dirección de cada site o e-mail la red se guía por el camino necesario para llegar a destino.

Para conectarse a la red es indefectible, en primer término, tener acceso a una computadora personal y que esta se encuentre provista de un elemento denominado módem[7]. Paso seguido, para tener acceso a Internet es necesario contratar los servicios de un ISP[8] (Internet Service Provider/Proveedor de Servicios de Internet), estas empresas se encuentran provistas de licencia para autorizar el uso de la red, funcionando de "puente" entre los usuarios y la red de redes.

Es decir, si Internet es equivalente a una autopista de información (information superhighway), los ISP juegan el rol de calles locales de acceso a la red. Por ello, cuando un usuario contrata los servicios de un ISP, este no se encuentra simplemente conectado a Internet, sino que pasa a ser parte de la red de redes.

La simple conexión de dos computadoras no produce efecto alguno, si esta conexión no se encuentra acompañada de un mismo lenguaje de comunicación. Es por ello, que existen infinidades de idiomas o programas para un entendimiento en el intercambio de datos entre dos computadoras. Estos idiomas son denominados protocolos (protocols); los dos lenguajes más importantes y mayormente usados en Internet son: TCP/IP[9] (lenguaje entre computadora a computadora) y HTTP (lenguaje de hombre a hombre).

Internet está provista de determinadas herramientas informáticas para el uso de esta fuente de comunicación y transmisión de datos; sintéticamente las más importantes hoy en día son las siguientes:

E-Mail (Correo Electronico)
Internet Relay Chat –IRC- (Grupos de Chateo)
Usenet Newsgroups
World Wide Web (W.W.W)

De las herramientas de comunicación que provee Internet, hoy en día, la mayormente utilizada es el denominado Correo Electrónico (Electronic Mail o E-Mail). Este particular correo puede ser equiparado a enviar una carta,

---

[6] Una conexión entre dos computadoras lograda a través de líneas telefónicas comunes y un módem. La mayoría de las personas que se conectan a Internet desde sus residencias lo hacen utilizando líneas conmutadas.

[7] Circuito para el ingreso y egreso de datos por intermedio de la red telefónica. Tiene por función conectar dos computadoras o más a través de la red telefónica existente. El nombre surge de una versión resumida de "Modulator/Demodulator" (Modulador/Demulador), una descripción algo técnica de como trabaja. El módem tiene la función de convertir señales digitales que envía el computador en sonidos análogos que pueden viajar a través de la red telefónica para ser luego interceptados y decodificados por otro módem. Estos sonidos son los extraños ruidos que uno escucha al conectarse a Internet.

[8] Al respecto corresponde efectuar la diferencia existente entre un proveedor de servicios de Internet y un proveedor de servicios On-line. El primero de ellos tiene la característica de proveer acceso a Internet a usuarios. A diferencia, el segundo no solo provee acceso sino que además posee su propio servidor para "vender" espacios tanto a usuarios como a empresas.

[9] Ver # 1 - TCP/IP: Protocolo de Control de Transmision (Transmission Control Protocol/Internet Protocol)

Es el protocolo principal para la comunicacion a traves de internet. Funciona mediante la division de informacion en pequeños paquetes que son enviados a traves de la red.

con la particularidad de que utiliza medios informáticos para su envío.. El Correo Electrónico permite a los usuarios transmitir mensajes entre dos o más personas alrededor del mundo.

Otra herramienta que día a día se encuentra en creciente expansión es Internet Relay Chat –IRC- o mejor conocido como "grupos de chateo" o chat rooms, estos tienen la particularidad de permitir dialogar en tiempo real con otros navegantes.

Por su parte, los "Newsgroups" son bases de mensajes agrupados por tema, permitiendo a los usuarios leer y enviar mensajes en cualquier momento y al grupo temático que el usuario desee. Al presente existen mas de 15.000 diferentes tópicos.

Por último, la más conocida de las herramientas que componen Internet, revolucionaria de las comunicaciones, es la "World Wide Web" (W.W.W.). Este método de comunicación permite a los usuarios publicar documentos, imágenes, videos, etc, pudiendo ser accedidos por cualquier otro usuario ubicado en cualquier otra parte del mundo.

De manera figurativa podemos asimilar a la W.W.W. a una gran librería, donde cada libro de esta librería virtual es denominado sitio y a su vez cada libro (sitio) tiene páginas interligadas que lo integran, creando esta infinidad de libros la denominada red de redes o W.W.W.

Las páginas o sites, pueden ser caracterizados como grupos de información que pueden ser colocadas en cualquier servidor (server), es decir, que el servidor donde el usuario desea tener su página puede estar ubicado en Tailandia mientras que el usuario tiene residencia en Argentina. Esta libertad de ubicación de páginas ha dado origen a infinidades de cuestionamientos e incertidumbre en el campo de la tributación, que trataremos de analizar a continuación.

4. LOS PROBLEMAS DE IMPOSICION EN LAS TRANSACCIONES COMERCIALES EFECTUADAS A TRAVES DE INTERNET (E-COMMERCE)

Por medio de Internet se ha creado un fenomenal canal de comercialización, ya que permitió no solo a las grandes, sino también a las medianas y pequeñas empresas llegar a mercados y, consecuentemente, potenciales consumidores, lo que sería de casi imposible logro sin este canal comercial.

Este fenómeno ha acortado distancias y ha hecho desaparecer fronteras, pasándose a convertir el mundo en un sólo mercado potencialmente accesible para todos y cada uno de los oferentes de productos y servicios.

Los efectos que acarrea el Comercio Electrónico a nivel mundial repercuten ineludiblemente en el campo de la tributación tanto nacional como internacional, surgiendo serios cuestionamientos en la forma de imposición no solo sobre los impuestos que basan su gravabilidad en la renta sino también sobre los impuestos al consumo.

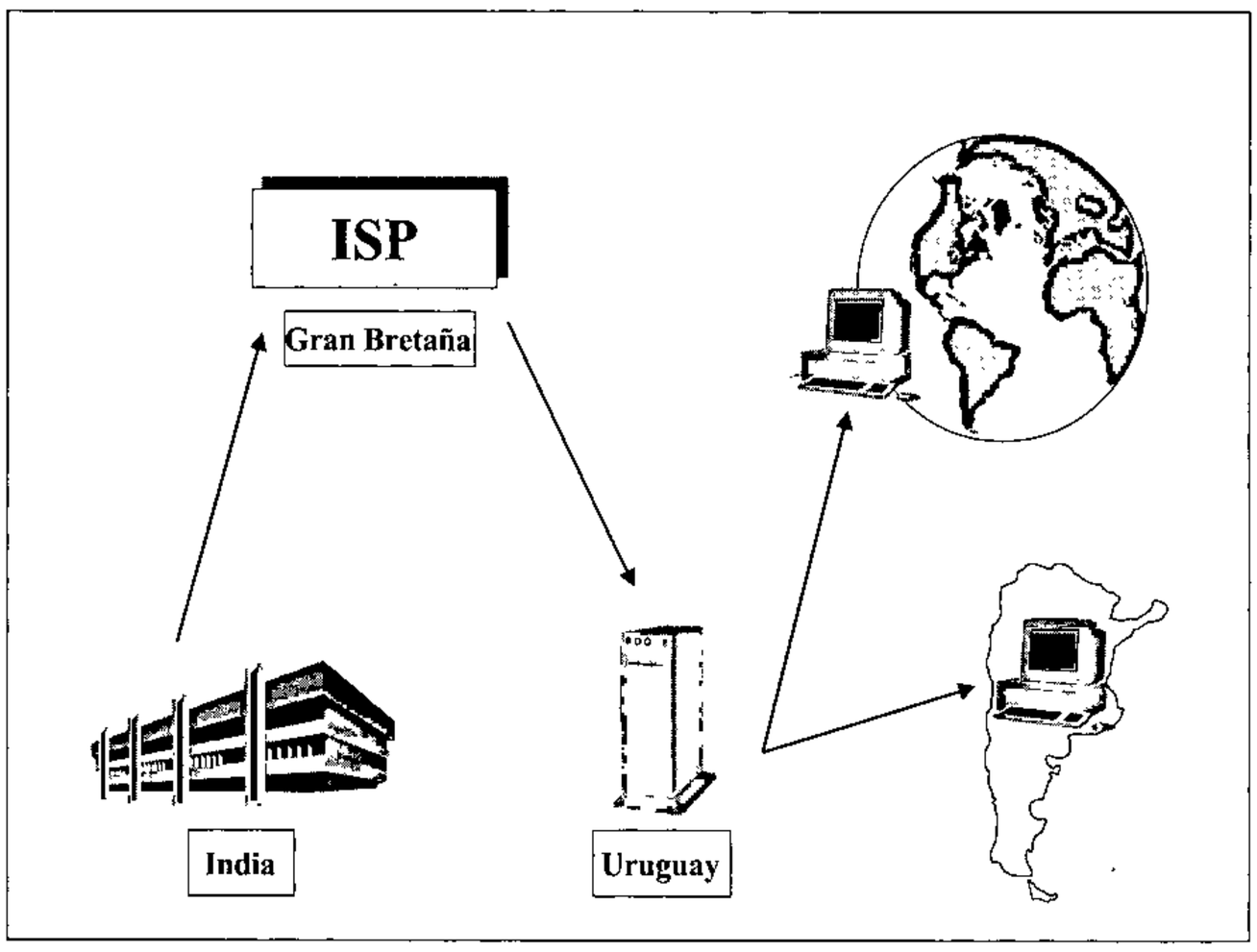
Para evaluar la magnitud del problema de imposición que genera las operaciones realizadas a través del Comercio Electrónico (E-Commerce) es menester efectuarse un mero cuestionamiento: ¿QUE ESTADO O JURISDICCION TIENE POTESTAD TRIBUTARIA SUFICIENTE PARA GRAVAR LAS TRANSACCIONES EFECTUADAS A TRAVES DE INTERNET?.

Esta simple pregunta es la detonadora de los principales problemas de imposición que hoy el mundo de la tributación se encuentra analizando y evaluando.

Para comprender la magnitud de la cuestión hemos desarrollado ciertos ejemplos:

Una empresa con sede en India, lugar donde ésta tiene exclusivamente la administración, contrata con un ISP (Internet Service Provider) de Gran Bretaña colocar una página (site) en un servidor ubicado en Uruguay, para efectuar operaciones de venta de downloading de música (el producto se baja en forma directa desde la página a la computadora personal del comprador) en Argentina y resto del mundo (Diagrama I).

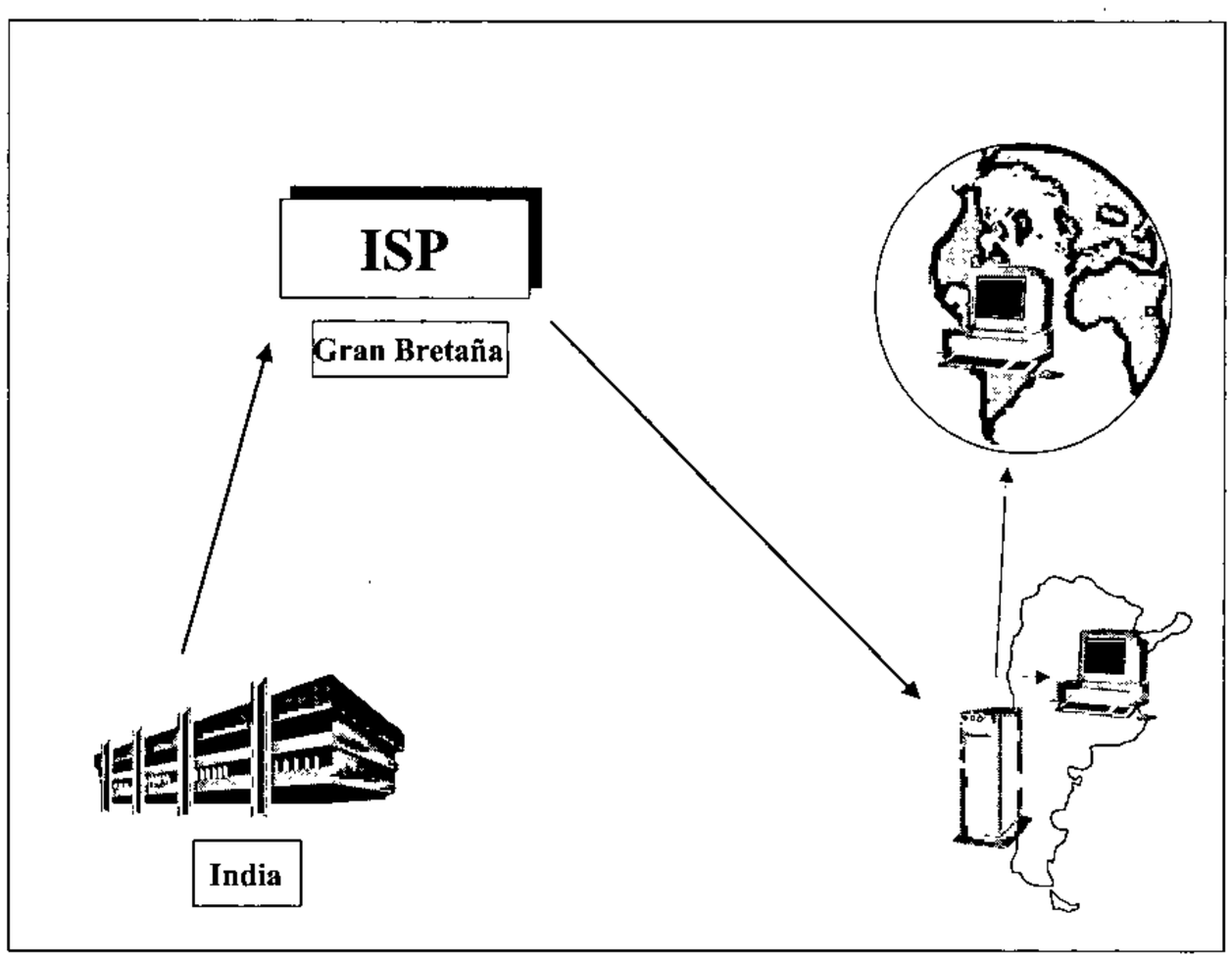
DIAGRAMA I



Es decir, que las autoridades argentinas se encontrarán con un sujeto del exterior que realiza operaciones comerciales habituales con sujetos ubicados en nuestro país. ¿Donde fue realizada la operación?, ¿qué jurisdicción tendrá potestades tributarias para gravar la operatoria? Respuestas posibles: 1) India, 2) Gran Bretaña, 3) Uruguay, 4) Argentina.

Tomemos similar caso pero, eventualmente, consideremos que el server se encuentra en Argentina (Diagrama II).

DIAGRAMA II



Las operaciones concertadas a través de ese servidor, ¿generarían renta imponible en Argentina?; ¿nos encontraríamos frente a un establecimiento estable?; ¿podría ser considerada una mera computadora (Server) como un establecimiento estable?; en caso de ser considerado un establecimiento estable, ¿ quién sería el sujeto obligado al ingreso de los gravámenes correspondientes?; estas ventas realizadas en Argentina, ¿estarían alcanzas por los Impuestos al Valor Agregado, sobre los Ingresos Brutos, o de Sellos?.

4.1. El Problema de la Potestad Tributaria en las Transacciones Internacionales –Criterios de Imposición.

El primero y más complejo de los cuestionamientos de difícil respuesta es el determinar cuál de los Estados intervinientes tendría potestades tributarias para gravar las operatorias realizadas a través de Internet.

Este es un problema que tiene sus orígenes desde los inicios de la tributación y de las transacciones a nivel mundial, hoy acentuado en virtud de la simplicidad y cantidad de transacciones que traerá aparejada esta nueva herramienta de comercialización.

La potestad tributaria puede ser definida como la facultad que tienen los Estados de crear unilateralmente tributos, cuyo pago será exigido a las personas sometidas a su competencia tributaria espacial. Esto, en otras palabras, importa el poder coactivo estatal de compeler a las personas para que le entreguen una porción de sus rentas o patrimonios, cuyo destino es el de cubrir las erogaciones que implica el cumplimiento de su finalidad de atender necesidades públicas[10], siempre que se encuentren bajo su ámbito espacial de imposición.

Cuando se lleva a cabo una transacción de carácter internacional, por lo general, los gobiernos de ambas partes involucradas en el acuerdo poseen, ya sea aplicando los principios de fuente, nacionalidad o residencia, potestad suficiente para ejercer individualmente su potestad tributaria sobre la operatoria.

Esta superposición de potestades tributarias puede traer como consecuencia una doble imposición de carácter tributario, reconocida mundialmente como el principal problema que enfrentan las transacciones internacionales. El único remedio posible para solucionar esta dificultad es una coordinación de carácter internacional, por medio de tratados, adecuación de legislaciones nacionales u Organismos Internacionales de Coordinación Tributaria.

Cada país conforma su propio sistema tributario regulando el tratamiento de las operaciones realizadas en el extranjero por los residentes del mismo, como así también las operaciones realizadas por extranjeros en el territorio de su jurisdicción. El sistema tributario internacional varía de país a país; sin embargo uno puede encontrar ciertas similitudes entre los diferentes sistemas. Ciertamente los tratados internacionales de carácter tributario son parte de esas similitudes regulando las bases para la determinación del impuesto a ingresar; otras veces es la propia legislación del país la que determina el apropiado tratamiento impositivo.

Generalmente los países ejercitan su poder jurisdiccional basándose en los principios de residencia o nacionalidad. En el campo tributario, el país ejercerá su jurisdicción sobre aquellas rentas obtenidas por los sujetos o compañías que estén establecidos en dicho. En la República Argentina el ejercicio del poder jurisdiccional recae no sólo sobre rentas que los ciudadanos o compañías residentes obtienen en el país sino también sobre las ganancias obtenidas en el exterior. Ejemplo, las ganancias obtenidas por una sociedad o un sujeto residentes argentinos por sus actividades desarrolladas en Italia se encontrarán sujetas al pago de impuesto en Argentina.

El principio de residencia justifica el ejercicio del poder tributario basándose en la teoría que los contribuyentes deben soportar el costo de llevar adelante la economía del país donde estén desarrollando su propia actividad. Por ejemplo, el país A ejerce su jurisdicción sobre el sujeto con nacionalidad del país B, si ese sujeto es considerado residente bajo la legislación del primer país.

---

[10] Hector B. Villegas, "Curso de Finanzas, Derecho Financiero y Tributario", Ed. Depalma, 1994, pág. 186.

Ciertos países no solo ejercitan su poder tributario basándose en la residencia de los sujetos, sino que hacen uso del principio de nacionalidad. El principio de nacionalidad sobre las personas físicas tiene gran similitud al principio de territorialidad. En ambos casos, es la conexión del sujeto con el país la que justifica el poder tributario ejercido sobre los mismos. Respecto del principio de la nacionalidad, esa conexión es de carácter legal, ya sea una sociedad o una persona física. Por su parte, cuando trata de territorialidad, la conexión es de hecho (donde ese sujeto es residente).

El poder tributario basado en el principio de la nacionalidad podría encontrar su justificativo en los beneficios que obtiene el ciudadano por encontrarse bajo la nacionalidad del país. Los ciudadanos americanos se encuentran "asegurados"; estos pueden retornar a su país cuando ellos lo dispongan, así mismo se encuentran protegidos por el gobierno de los Estados Unidos en cualquier parte del mundo. El cumplimiento de los deberes tributarios contribuye a la sustentación del mencionado seguro. Las compañías norteamericanas, si bien su lugar físico no es el propio país, gozan de los beneficios de la protección de las leyes americanas.

Otro principio en que los sistemas tributarios mundiales encuentran fundamentación para el ejercicio de su poder tributario es el principio de la fuente o territorialidad. Este principio no tiene en cuenta la residencia o nacionalidad, ya que su basamento es el lugar de producción de la renta, sin importar si el sujeto es ciudadano o residente del país. Por ejemplo, cierto país impondrá la obligación del pago de tributos a aquella renta obtenida por no residentes, por los negocios desarrollados en su jurisdicción.

Ahora bien, la aplicación de estos distintos principios lleva a la consecuencia inevitable de la doble imposición. Por ejemplo, el país A ejerce jurisdicción tributaria sobre un determinado sujeto, basándose en la nacionalidad o residencia de dicho contribuyente; mientras que las ganancias obtenidas por el mismo sujeto en el país B se encontrarán alcanzadas en dicha jurisdicción. Para solucionar esta situación, la Argentina en particular y la gran mayoría de los países de América como del continente Europeo persiguen la política de sobreponer el primario poder tributario, es decir, donde la ganancia fue obtenida (principio de la fuente), por sobre el principio de residencia o nacionalidad. De ésta manera, nuestro país, por lo general, otorga a sus residentes un crédito fiscal por aquel impuesto pagado en otro país por las rentas obtenidas en dicho país.

4.2. El Concepto de "Establecimiento Permanente" para la Ley Argentina

Bajo el análisis de estos principios no se puede obviar el concepto de "Establecimiento Permanente"; este criterio reconoce efectos fiscales ante el hecho de desarrollar actividad económica en un lugar que no es el domicilio, residencia, o nacionalidad del contribuyente[11]; basándose en un razonamiento adecuado a los tiempos presentes, otorga preeminencia al lugar donde los sujetos efectúan su actividad económica por sobre la nacionalidad o residencia de estos.

Este criterio es el de mayor relevancia y es el que hoy en día se encuentra en discusión y eventual análisis en los mayores países del mundo[12]. Discusión que versa, en nuestro caso, sobre la posibilidad o no de encuadrar a los (Proveedores de Servicio de Internet (ISP), servidores (servers) o páginas web (sites) bajo este concepto.

El porqué de esta discusión encuentra respuesta en las previsiones dispuestas en la mayoría de los Convenios de Doble Imposición al disponerse en ellos la no posibilidad de imposición sobre una persona física o jurídica no residente, excepto que exista un establecimiento permanente en ese Estado.

---

11 Carlos M. Giuliani, "Derecho Financiero", Tomo I, 6° Edición, Editorial Depalma, Pág. 405.

12 Uno de los más resonantes casos fue el "Pipeline Case" del Tribunal Fiscal Federal de la República de Alemania, de fecha 30 de octubre de 1996, en el cual se ha dispuesto que "...el uso con propósitos de negocio, significa el desarrollo de una actividad de negocio (...). Este requerimiento fue satisfecho en el presente caso, porque el transporte de petróleo crudo a través de un oleoducto es un negocio. El empleo de personas (Hombre de negocios, empleados, personal de un contratista o subcontratista) trabajando en la base no es necesario en ningún caso; es suficiente, particularmente en el caso de instalaciones automáticas, si el hombre de negocios lleva a cabo su actividad a través de la base (instalaciones)...".

Por ello y en virtud de la necesidad de todo Estado de no "ceder" jurisdicción fiscal, repercutiendo en una disminución en orden a su recaudación, es que hoy en día la mayoría de los países importadores de capital se encuentran estudiando la posibilidad de encuadrar, ya sea los ISP, servidores o, en su caso, "páginas web", dentro del concepto de establecimiento permanente.

El concepto de establecimiento estable siempre fue ambiguo en nuestra legislación, ya que no existía norma en la Ley del Impuesto a las Ganancias que encerrase la conceptualización de dicho precepto. La reforma introducida por la Ley 25.063, incorporó (Artículo 128, segundo párrafo) una definición de establecimiento estable, disponiendo que *"...son las organizaciones en forma de empresa estable para el desarrollo de actividades comerciales, industriales, agropecuarias, extractivas o de cualquier tipo, que originen para sus titulares residentes en la República Argentina ganancias de tercera categoría. La definición precedente incluye a las construcciones, reconstrucciones, reparaciones, y montajes cuya ejecución en el exterior demande un lapso superior a 6 (seis) meses, así como los loteos con fines de urbanización y la edificación y enajenación de inmuebles bajo el régimen similar al establecido por la ley 13.512, realizados en países extranjeros"*.

Si bien la normativa transcripta fue prevista para situaciones en que los sujetos residentes en el país efectúen operaciones en el exterior a través de la titularidad de estos establecimientos, a falta de definición para el supuesto contrario, sería eventualmente aplicable ya que Ley del Impuesto no efectúa una remarcada diferenciación en los términos utilizados en ambos supuestos.

En virtud de ello, podemos sostener que los "establecimientos permanentes" de sujetos radicados en el exterior deben tener como características principales, las siguientes:

1. Que se trate de una Organización
2. Que conforme una empresa
3. Que sea estable o permanente

Estos caracteres necesarios para la presencia de un establecimiento permanente, implican la existencia de una dirección, una estructura estable, un patrimonio[13] y un lugar físico con el fin de llevar a cabo una actividad comercial o de otro tipo. Es decir que el establecimiento debe tener todos los elementos necesarios para desarrollar de forma autónoma una actividad, pudiendo, de esta manera, ser considerado como un "lugar de negocios" "independiente" del principal.

4.3. El concepto de establecimiento permanente para la OCDE y sus implicancias en el Comercio Electrónico

La definición de establecimiento permanente propuesta por la OCDE (Organización de Cooperación y Desarrollo Económico), en el Modelo de Convenio para evitar la Doble Imposición -que data del año 1963 introduciendo algunas variaciones en los años 1977 y 1992- es la utilizada en la mayoría de las Convenciones Internacionales firmadas por los diferentes países alrededor del mundo.

Específicamente el artículo 5 del Modelo Convenio dispone como base para su conceptualización, que la expresión establecimiento permanente significa, a los fines del Convenio, un lugar fijo de negocios mediante el cual una empresa realiza toda o parte de su actividad.

Al respecto el 8 y 9 de Octubre de 1998, en una conferencia llevada a cabo en Ottawa por la OCDE, se ha propuesto una modificación al concepto de "establecimiento estable" que prevé el artículo mencionado, con la finalidad de adaptarlo a las operaciones realizadas a través de Internet.

---

13 Vives, María Luisa "Principios para determinar la renta y el capital de establecimientos permanentes: su aplicación a entidades financieras y a compañías de seguros" D.T., T.XIV, pag. 34.
Raimondi, Carlos y Atchabahian, Adolfo, "El Impuesto a las Ganancias", Editorial Depalma, Pág. 365.
Gotlib, Gabriel, "Un concepto tributario fundamental al exportar: Establecimiento permanente" PET, 30/06/97, pag. 13.

La propuesta tiene sus bases en el estudio de las características de los "servers" para encuadrarlos en el concepto de "establecimiento estable". Como hemos expuesto precedentemente, los servers son computadoras sobre las cuales reside la información que conforma una página (sitios) de Internet.

La OCDE tiene como criterio que, cuando una empresa ejerce actividades en dos países, esta va a tributar por las utilidades obtenidas en razón a su actividad exclusivamente en el país de residencia, excepto que la empresa tenga un establecimiento estable en el otro país[14].

En virtud de este criterio el grupo de trabajo de la OCDE que se encuentra en estudio de las implicancias del Comercio Electrónico en la tributación internacional, presentó -en la mencionada asamblea- una propuesta de reforma del artículo 5° del Convenio. El propio trabajo advierte que no debe considerarse como la opinión de la OCDE, ni la de sus países miembros[15], sino que su contenido tiene como finalidad recibir comentarios y opiniones, comprometiéndose a sellar una primera postura en la asamblea de febrero del 2000.

La propuesta introduce nuevas consideraciones sobre los servidores. En primer término aclara que las páginas no envuelven elemento tangible alguno, no pudiendo constituir, por sí sólas, un "lugar de negocios"; afirmando que sólo el software y la información consultada es lo que importa de la página. Por otra parte, el server por el cual aquella página es operada, es una pieza del equipo que necesita una locación física y ello podría ser considerado o podría constituir el "lugar de negocios" de la empresa que opera en ese país.

Esta distinción podría ser considerada importante ya que, por lo general, la empresa que opera el servidor en el cual se encuentra la página, difiere de la compañía que presta servicios o comercializa los productos (ver DIAGRAMAS I y II anteriores). Ello permitiría decir que, en tanto la compañía que presta un servicio o comercializa un producto no es dueña del servidor en el cual se sitúa la página, no podría configurarse el "lugar de negocios"; ya que no existiría una presencia física de esta compañía, no existiría activo tangible alguno.

Otro de los temas analizados es si el ISP (Internet Service Provider) podría llegar a ser considerado un agente, derivando consecuentemente en un establecimiento estable. El ISP es la empresa que provee el acceso a Internet, asimismo sitúa páginas de diferentes empresas en sus propios servers. En virtud de esto último, surge el cuestionamiento de si es posible considerar a los ISP como establecimientos estables de aquellas empresas que colocan las páginas en sus servidores. Por cierto que la falta de poder para contratar en nombre de éstas empresas no haría posible dar este carácter a los ISP.

4.4. Los principios generales de tributación en el Impuesto a las Ganancias Argentino y su aplicación sobre las transacciones efectuadas a través de Internet

El sistema tributario rentístico en nuestro país se encuentra basado fundamentalmente en el principio de residencia, conocido actualmente como "de la renta mundial", siendo complementado por el principio de la fuente o territorialidad y teniendo en cuenta el elemento de "establecimiento estable/permanente".

En el origen, el Impuesto a las Ganancias estaba basado en el criterio de la fuente, teniendo por finalidad gravar exclusivamente aquellos beneficios obtenidos en el territorio de la Nación, ya sea por sujetos radicados en el país o fuera de él. Posteriormente, en el año 1992 por medio de la reforma introducida por la Ley 24.073, se optó por ampliar la base de imposición que se venía aplicando, adoptándose el principio de renta mundial para los residentes en el país. De esta manera, se dejó atrás la concepción de gravar exclusivamente las rentas obtenidas en nuestro país, pasando a incluir dentro del objeto del impuesto a las rentas obtenidas en el exterior por sujetos residentes en nuestro país. Sin perjuicio de ello, se mantuvo el criterio de la fuente para todos aquellos sujetos no residentes en el territorio argentino.

---

[14] Artículo 7 (Modelo de Convenio – OCDE)

[15] Países Miembros de la OCDE: Australia, Austria, Bélgica, Canadá, República Checa, Dinamarca, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Irlanda, Italia, Japón, Corea,, Luxemburgo, México, Holanda, Nueva Zelanda, Noruega, Polonia, Portugal, España, Suiza, Suecia, Turquía, Estados Unidos de América, Reino Unido.

El artículo 1°, segundo párrafo, de la ley del impuesto actualmente dispone que los sujetos residentes en nuestro país, ya sea personas físicas o jurídicas, tributarán sobre la totalidad de sus ganancias obtenidas tanto en el país como en el exterior; permitiendo, ante los problemas de doble imposición internacional que motiva este criterio de imposición, computar como pago a cuenta (tax credit) del impuesto, las sumas efectivamente abonadas por tributos análogos sobre sus actividades en el extranjero, hasta el límite del incremento de la obligación fiscal argentina originado por la incorporación de la ganancia obtenida en el exterior.

Por su parte, el criterio de la fuente previsto por el artículo 5° y tratado por el artículo 91, establece, para el supuesto de personas físicas o empresas residentes fuera de los límites de nuestro territorio (Beneficiarios del Exterior), que serán sujetos del impuesto toda vez que perciban rentas de fuente argentina. En caso de darse el supuesto comentado, el sujeto que realiza el pago al beneficiario deberá efectuar una retención del 35% de las ganancias netas e ingresarla al fisco.

Todos aquellos sujetos que perciban ganancias de fuente argentina en el extranjero, en forma directa o por intermedio de apoderado, agente, representante o cualquier otro mandatario en el país, toda sociedad constituída y domiciliada en el exterior, o quien las percibiese en el país, pero sin acreditar residencia estable en él, serán considerados a los efectos del impuesto beneficiarios del exterior.

Trasladando estos conceptos legales a las transacciones efectuadas a través de Internet, en principio no existiría cuestionamiento al sostener que, tanto aquellas personas físicas radicadas en el país, cuanto las sociedades y establecimientos estables comprendidos en el artículo 69 de la Ley del Impuesto a las Ganancias, deberán tributar en la Argentina por los beneficios que obtengan en relación a las transacciones que efectúen a través de la Red.

Ahora bien, el art. 69 de la Ley menciona como sujeto del impuesto a los establecimientos estables; y si bien previo a la ley 25.239 esta clase de sujetos debían tributar exclusivamente por las ganancias de fuente argentina (art. 126), al presente tributan por la totalidad de los beneficios obtenidos, es decir, tanto en el país como en el exterior (Renta Mundial).

Sobre la base del desarrollo expuesto en el punto 4.2 y señalado en párrafos precedentes, cabe preguntarse: ¿es posible considerar establecimiento estable a una página web (site) colocada en un server ubicado en nuestro país?

4.4.1. A efectos de responder a esta cuestión, entendemos conveniente efectuar ciertas diferenciaciones respecto del tratamiento a otorgar, en relación a las posibles operaciones a realizar a través del mismo. Es decir, se debe prestar especial consideración a la conformación técnica del site entendiendo que, para el supuesto que se reúnan conjuntamente las siguientes funciones: A) concertar ventas, B) receptar pagos, y C) programar el envió de mercadería a través del site; estaríamos frente a un establecimiento estable, ya que la propia web, sin perjuicio de la falta de intervención humana directa, realizaría todas las funciones propias de una organización empresaria.

Por su parte, en el supuesto que el server donde se encontraran colocadas las páginas no fuera de propiedad del sujeto que posee el dominio del sitio, se generaría una falta de presencia física del sujeto en el territorio; por cierto que con la ausencia de este elemento no podría configurarse un "lugar de negocios", y el consecuente encuadre bajo el concepto de establecimiento permanente.

Siguiendo la misma línea de razonamiento, entendemos que las transacciones efectuadas por páginas colocadas en servidores ubicados en nuestro país que NO cumplimenten las funciones descriptas precedentemente (Ventas, recepción de pagos y orden de envío al comprador) no conformarían las características necesarias para encuadrarlas bajo la conceptualización de "establecimiento estable" prescripta en la Ley del Impuesto a las Ganancias.

No obstante ello, en razón de las infinidades de productos y servicios que pueden ser ofrecidos a través de la red, correspondería verificar en cada caso concreto los condicionamientos técnicos que conforman el site para precisar su encuadramiento bajo los términos de establecimiento estable dispuestos por la normativa argentina.

El razonamiento que venimos delineando no puede obviar que las operaciones comerciales efectuadas a través de Internet son -por lo general- transacciones de carácter internacional y, como tales, en esta clase de operaciones no sólo operan normas de carácter nacional sino también aquellas pertenecientes al ámbito internacional (Convenios Internacionales) y legislaciones de los intervinientes países donde se encuentran radicados los sujetos participantes de la transacción.

Es por ello que debe prestarse suma atención a los sujetos y países intervinientes para determinar el tratamiento tributario a imprimir a las transacciones efectuadas a través de la Red, evaluando la existencia o no de tratados de doble imposición entre las jurisdicciones intervinientes[16].

Este precepto nos lleva a sostener que, en el supuesto que las páginas web de propiedad de un residente extranjero, colocadas en un server ubicado en nuestro país, sean consideradas establecimiento estable, debiendo tributar por los beneficios obtenidos por operaciones realizadas en nuestro país y en el exterior.

Por su parte, en lo que respecta a sujetos residentes en el exterior que utilicen la red de redes para insertarse en nuestro mercado, en principio, tributarán exclusivamente por los beneficios netos de fuente argentina que obtengan de aquellas transacciones.

4.4.2. En el supuesto que el dominio del site se encuentre en manos de un "Beneficiario del Exterior", es menester analizar el eventual y disímil tratamiento impositivo que tendrán las transacciones y su tratamiento en el Impuesto a las Ganancias, en relación al objeto que persigan las mismas.

En este sentido, puede advertirse que la Ley del Impuesto a las Ganancias (art. 8, inc, b) considera renta de fuente extranjera a los ingresos de productos a la Republica por exportadores extranjeros. Es evidente que esta norma previó la no gravabilidad de importaciones efectuadas por sujetos ubicados en nuestro país, considerando los bienes importados como de propia producción del importador, debiendo gravarse los beneficios netos que se obtengan de las ventas que se efectúen con posterioridad sobre estos productos.

El problema que hoy vemos con las transacciones efectuadas a través de la Red es que una gran cantidad de "importadores" van a ser consumidores; es decir, que el comercio electrónico eliminará las etapas de intermediación de productos, pasando, de ésta manera, los bienes a ser vendidos en forma directa por los propios productores a consumidores radicados en cualquier parte del mundo. Por ello es de advertir que nuestra legislación no prevé la gravabilidad de este tipo de transacciones, por el contrario es la propia ley del impuesto que las excluye de su objeto[17].

Por su parte, cuando se trata de prestaciones o locaciones de servicios, la misma ley advierte (art.12) que las ganancias o beneficios obtenidos por honorarios u otras remuneraciones originados por asesoramiento técnico, financiero o de otra índole prestado desde el exterior, son de fuente argentina.

En virtud de ésta última norma mencionada, todo asesoramiento que encuadre en las previsiones de la ley deberá tributar el impuesto, debiendo el contratante del servicio efectuar la correspondiente retención e ingreso al fisco, sobre el total del precio pagado por éste considerando las presunciones de ganancias que la ley contempla. Como es de suponer, ante los servicios prestados a través de la Red, existirá en cabeza del consumidor una imposibilidad material de retención –en virtud de la composición de las páginas- sobre los pagos que éste efectúe al exterior; consecuentemente los ingresos al fisco se encontrarán a cargo del sujeto pagador, situación que traerá dificultades evidentes en la actividad de fiscalización que deberá enfrentar la Autoridad Fiscal.

---

16 Nuestro país tiene firmado 14 Convenio con diferentes Estados, si bien la mayoría de estos tratados persiguen los lineamientos del Modelo propuesto por la OCDE, ciertos otros como ser los firmados con Brasil, Bolivia, entro otros, guardan algunas peculiaridades.

17 Sin perjuicio de lo comentado, debemos advertir que la propia Direccion General Impositiva dispuso por medio de la Resolucion General N 3955 (modificada por la R.G. 3.964), un regimen de percepcion, cuyo receptor sera la Administracion Nacional de Aduanas (Hoy, Direccion General de Aduanas) en mérito a las atribuciones conferidas por el Decreto N 1.076/92. Este Regimen recae sobre las importaciones de bienes destinados a su comercializacion en el mercado interno, incluyendo las importaciones de bienes de uso no amortizables o aquellos bienes destinados al uso o consumo particular de quienes los importan.

Por último, corresponde mencionar aquellos bienes como ser software, música, libros, artículos, revistas, y demás productos, que se "bajan" en forma directa desde el server donde se encuentran colocados, a la computadora personal del consumidor.

El tratamiento a dispensar sobre la "baja de información" en forma de "bites", es una cuestión que hoy en día se encuentra en plena discusión a nivel mundial. La discusión versa sobre el carácter que se le debe dar a los productos vendidos y "entregados" a través de la Red. La primera postura sostiene que se debe aplicar similar tratamiento al producto como si hubiera sido una venta y "entrega" Off-line. Por otra parte, se critica ésta postura, aduciendo la imposibilidad de los gobiernos de determinar qué tipo de producto intervino en la operación, ya que el único rastro posible que le quedará a las autoridades es la cantidad de bites que la transacción demandó; por ello esta última postura brega por la unificación del tratamiento de estos productos bajo un mismo concepto, como ser la prestación de servicios.

Respecto a nuestra legislación nacional, podemos sostener que, al día de hoy, no existe tratamiento diferencial alguno por las operaciones realizadas o productos obtenidos en forma directa a través de la Red; por ello la imposición sobre los bienes y servicios obtenidos a través Internet tendrá el tratamiento que hoy prevé la Ley en cada caso en particular, aplicando las correspondientes exenciones cuando así corresponda o, en otros casos, empleando las presunciones que dispone la Ley en materia de fuente en razón al "producto- objeto".

No obstante ello, existe una inevitable diferencia entre la comercialización de bienes "tangibles" e "intangibles o servicios". Al tratarse de un bien tangible, el envío va a tener que seguir los canales normales de ingreso a nuestro territorio, e indudablemente nos encontramos frente a una importación. Por su parte, cuando se trata de bienes o servicios que pueden ser enviados por un canal virtual (baja de la red), parecería que el concepto de importación se debilita y consecuentemente la definición de la línea demarcatoria entre fuente argentina y extranjera se diluye.

4.4.3. En virtud del análisis efectuado en los párrafos y apartados precedentes, a continuación retomaremos los ejemplos planteados en el punto 4 del presente trabajo a efectos de evaluar el tratamiento a aplicar a las diferentes partes intervinientes:

Diagrama I:

La empresa radicada en India, por ser un sujeto radicado en el exterior y no poseer establecimiento estable en nuestro país, tributará como beneficiario del exterior. Consecuentemente, las personas físicas o jurídicas que realicen compras de música por intermedio de la página (site) de la empresa India deberán retener sobre el precio abonado el 17,5%[18].

Respecto de las demás partes intervinientes, no se encontrarán sujetos a retención u obligados de ingreso de gravamen alguno.

Diagrama II

Este supuesto se diferencia del Diagrama I por el sólo hecho de que el server se encuentra ubicado en nuestro país, con la particularidad de que la propiedad del server no está en cabeza de la empresa ubicada en India, sino de un ISP radicado en Gran Bretaña.

En virtud de la situación mencionada, la empresa radicada en India tributará de forma similar a la comentada en el Diagrama I.

---

18 *Por tratarse de bienes previstos en el artículo 13, la ley presume, sin admitir prueba en contrario, que constituye ganancia neta de fuente argentina el 50% del precio pagado a los productores, distribuidores o intermediarios por la explotación en el país de este producto. Sobre la base comentada debe retenerse el 35%.*

Por su parte, en razón de la ubicación del server (Argentina) podríamos sostener que el ISP radicado en Gran Bretaña será sujeto de impuesto en nuestro país, ya sea como consecuencia de configurarse los requisitos necesarios para encuadrar como establecimiento estable o como beneficiario del exterior, dependiendo de la actividad que realice el ISP en nuestro país, y la finalidad buscada por éste con el sever ubicado en nuestro territorio.

En el supuesto de no configurarse los elementos necesarios para encuadrar en el concepto de establecimiento estable, el ISP tributará como beneficiario del exterior, ya que las rentas provenientes de locación o explotación de bienes muebles (servidor) ubicados en nuestro país, son rentas alcanzadas por el impuesto a los efectos de nuestra Ley (art. 45 inciso b).

Ahora bien, en el presente caso, por haberse convenido los términos del acuerdo en el exterior y además el locatario no ser un sujeto inscripto en el impuesto a los efectos de nuestra Ley, existiría una complejidad manifiesta a efectos de la retención. Es decir que, si bien nuestra legislación entiende que los beneficios obtenidos por la locación de bienes muebles situados en el país son ganancias de fuente argentina, en virtud a los sujetos involucrados en la transacción existiría un problema a resolver respecto a la forma de cumplimiento de la obligación.

5- CONCLUSION

Como hemos podido observar a lo largo del presente trabajo, el número de transacciones efectuados por medio de Internet se encuentra en constante crecimiento, es por ello que la mayoría de los Estados-Naciones han percibido los consecuentes beneficios y eventuales perjuicios que generará en un futuro próximo esta nueva herramienta de comercialización en vista a la política tributaria que se adopte.

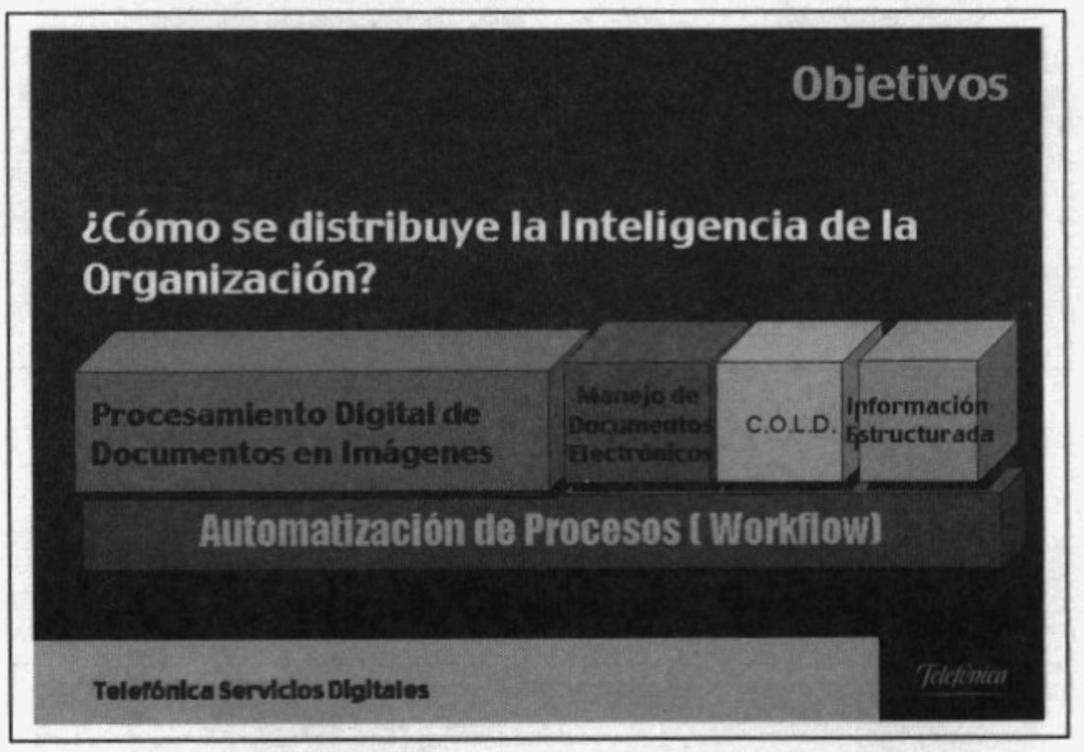
Por ello, los criterios vertidos en el presente trabajo constituyen pequeñas piezas que conformarán las distintas posturas que adoptarán las autoridades fiscales frente al inminente cambio en la forma de efectuar transacciones comerciales que impone Internet.

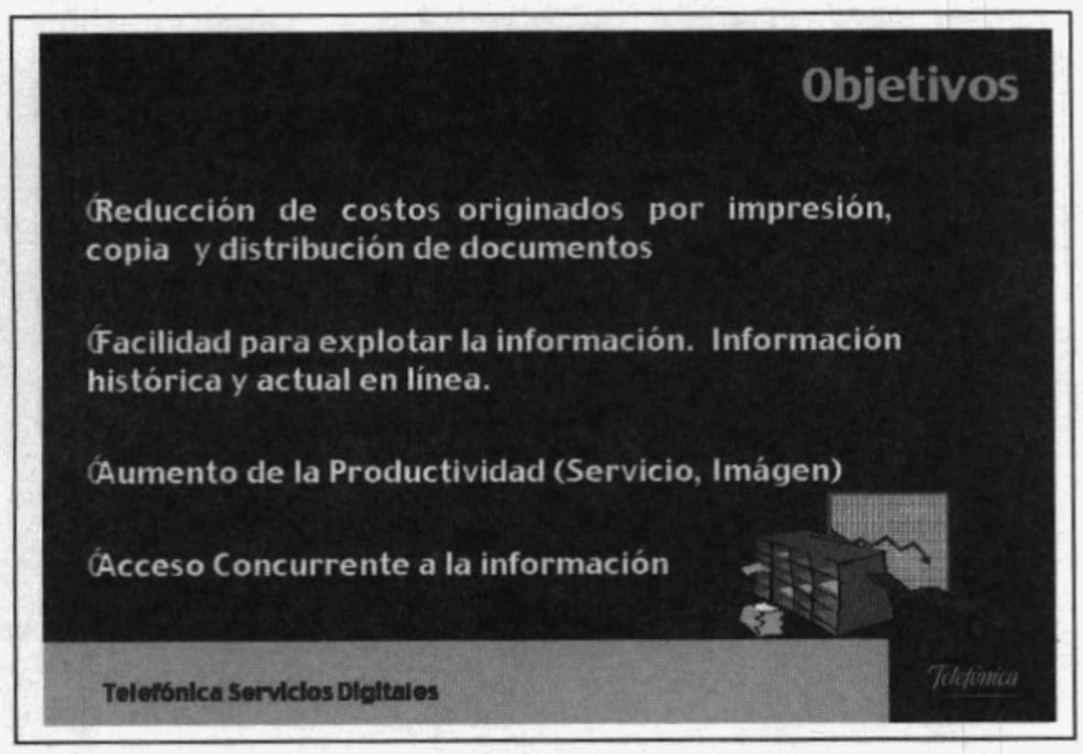
Estos criterios, que son discernidos ya en el nivel internacional, deberán ser evaluados por nuestros gobernantes, haciendo conciencia de que nuestra legislación reclama toda una reforma legislativa en búsqueda del menor menoscabo del nivel de recaudación nacional y en aras de la obtención de la equidad tributaria internacional en el E-Commerce y sus consecuencias.

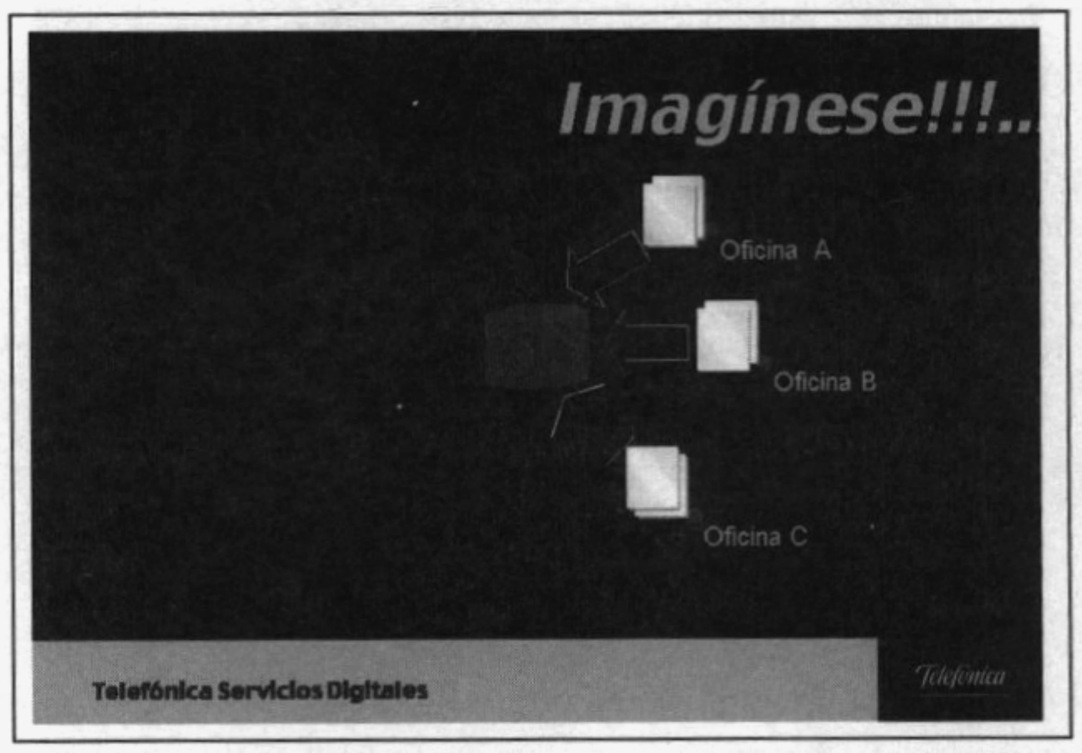
Aplicación de Tecnología y Derecho como un caso de Negocios Telefónica Servicios Digitales

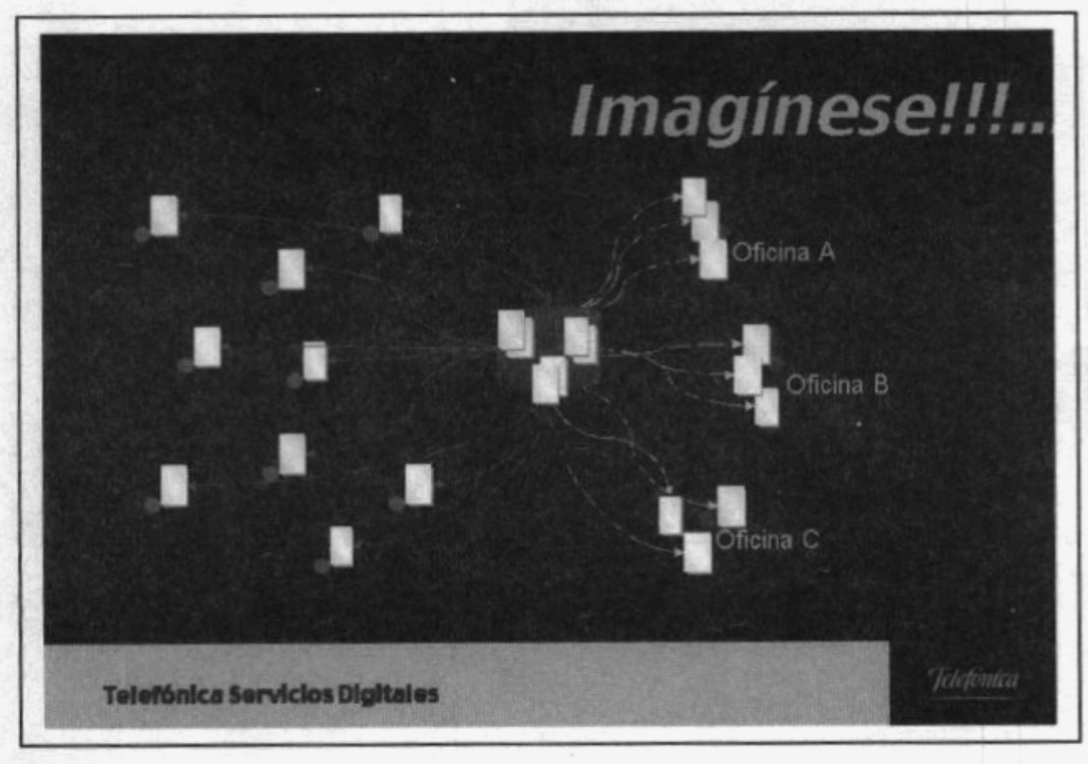
Richard Wadsworth Delgado
Gerente de Operaciones

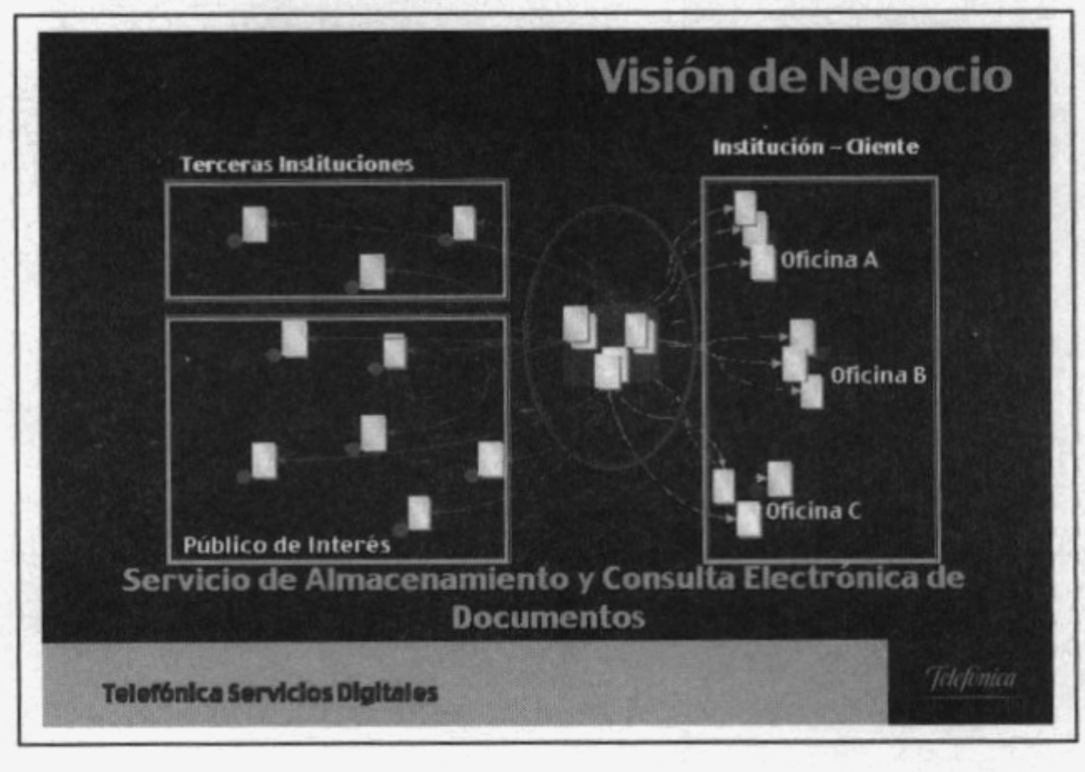


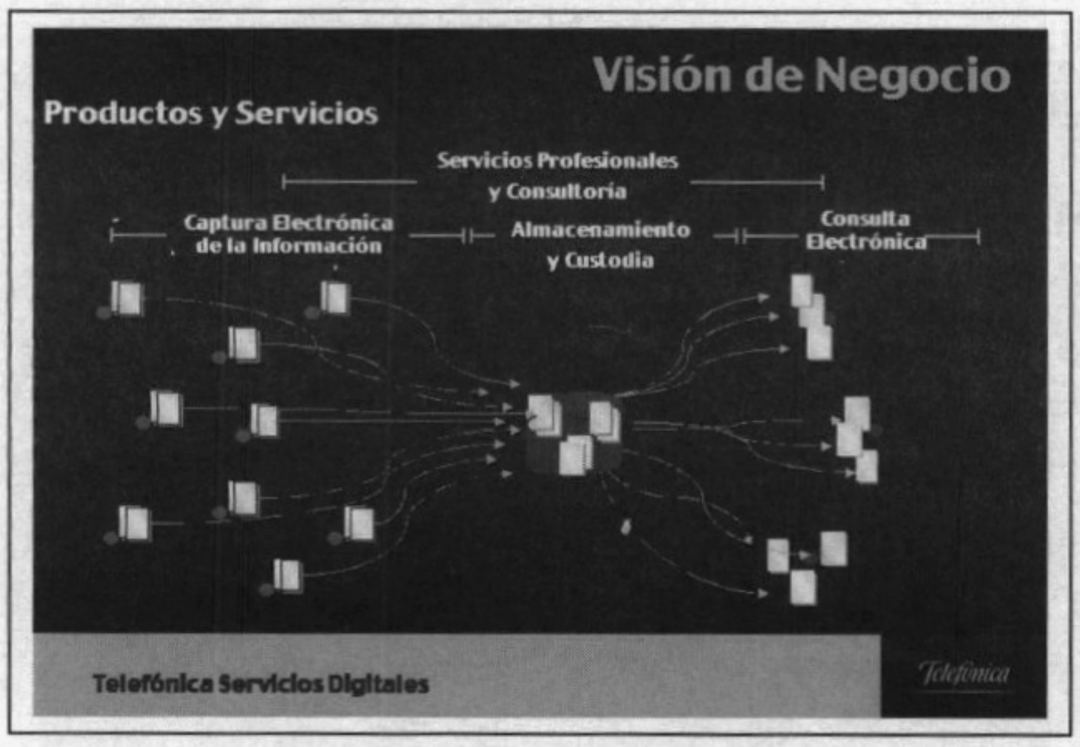


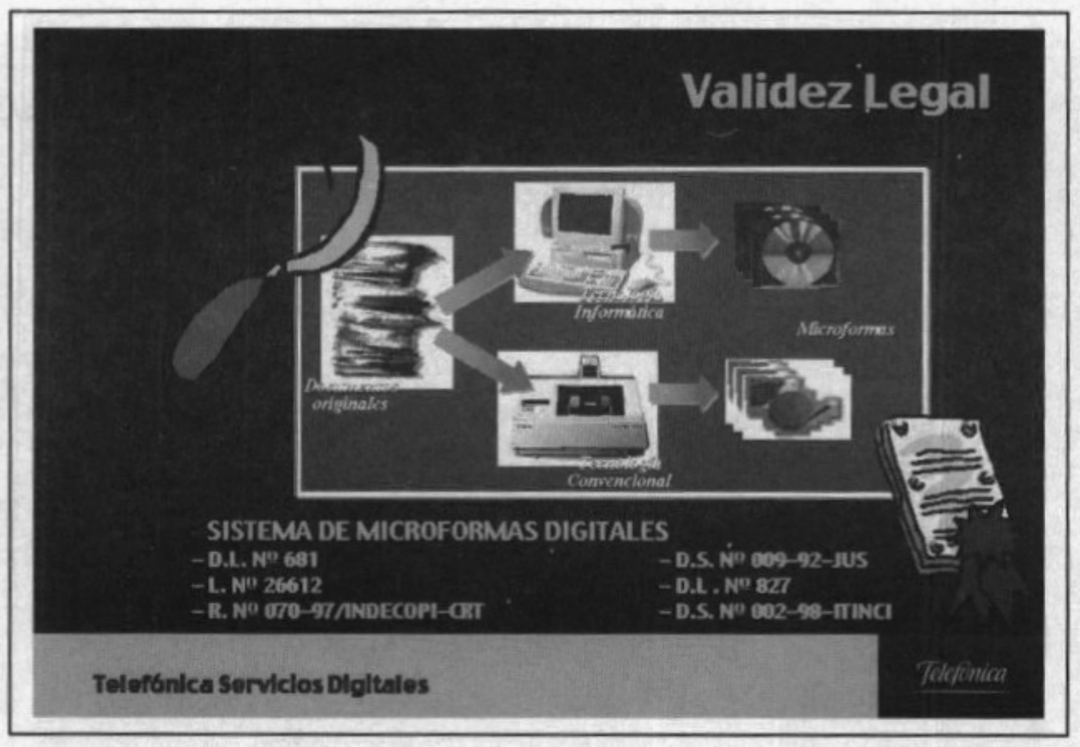


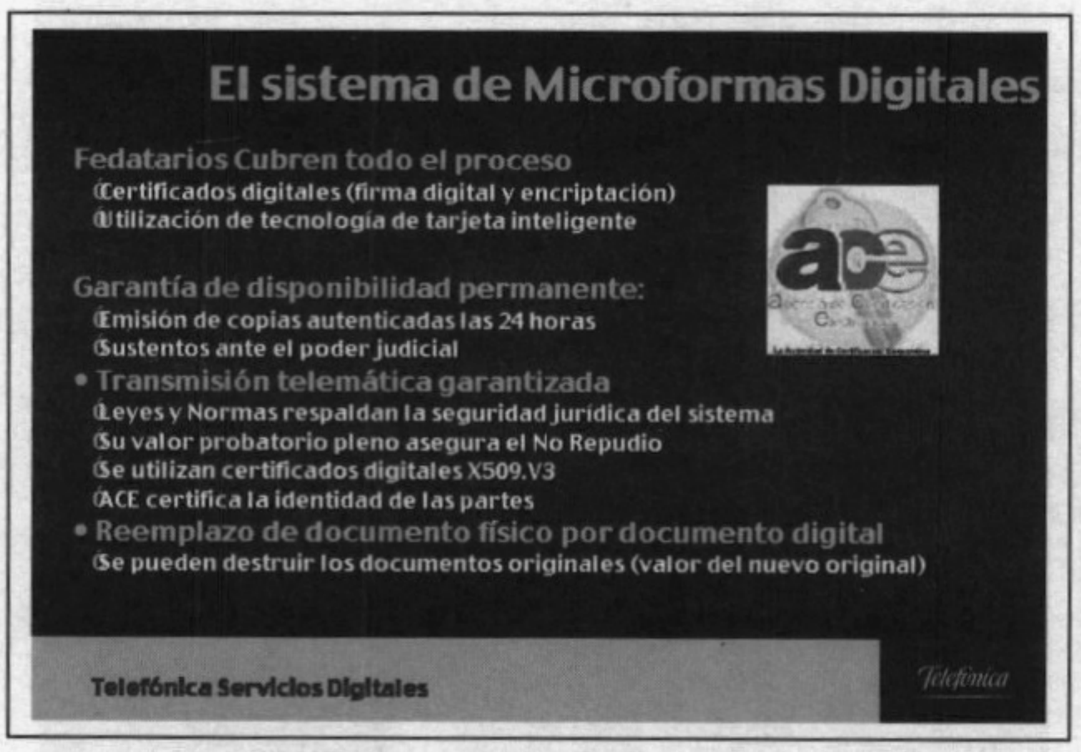




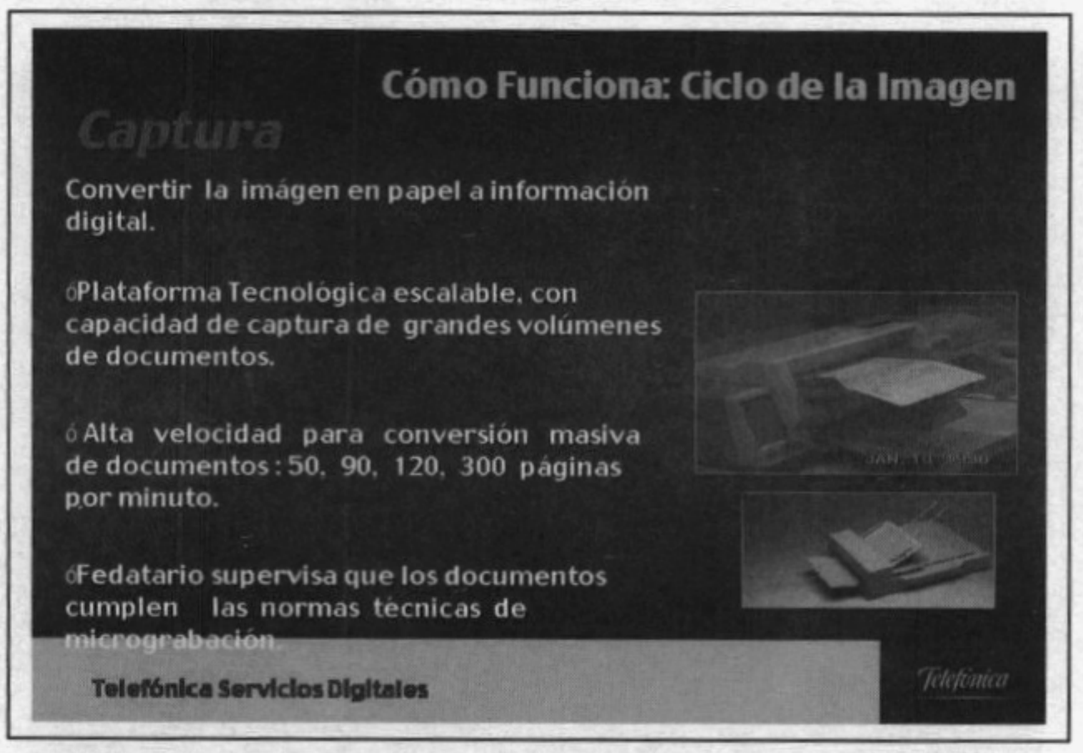



Visión de Negocio
Productos y Servicios
Servicios Profesionales y Consultoría
Captura Electrónica de la Información
Almacenamiento y Custodia
Consulta Electrónica
Telefónica Servicios Digitales
Telefónica


Validez Legal
Información
Microformas
Documentos originales
Tecnología Convencional
SISTEMA DE MICROFORMAS DIGITALES
– D.L. Nº 681
– L. Nº 26612
– R. Nº 070–97/INDECOPI–CRT
– D.S. Nº 009–92–JUS
– D.L . Nº 827
– D.S. Nº 002–98–ITINCI
Telefónica Servicios Digitales
Telefónica


El sistema de Microformas Digitales
Fedatarios Cubren todo el proceso
Certificados digitales (firma digital y encriptación)
Utilización de tecnología de tarjeta inteligente
Garantía de disponibilidad permanente:
Emisión de copias autenticadas las 24 horas
Sustentos ante el poder judicial
• Transmisión telemática garantizada
Leyes y Normas respaldan la seguridad jurídica del sistema
Su valor probatorio pleno asegura el No Repudio
Se utilizan certificados digitales X509.V3
ACE certifica la identidad de las partes
• Reemplazo de documento físico por documento digital
Se pueden destruir los documentos originales (valor del nuevo original)
Telefónica Servicios Digitales
Telefónica


Cómo Funciona: Ciclo de la Imagen
Consulta
Captura
Almacenamie
Indización
TSD cuenta con certificación de Idoneidad Técnica de Procesamiento de Microformas, los fedatarios juramentados en informática dan fe de cada uno de los procesos
Telefónica Servicios Digitales
Telefónica


Cómo Funciona: Ciclo de la Imagen
Captura
Convertir la imágen en papel a información digital.
Plataforma Tecnológica escalable, con capacidad de captura de grandes volúmenes de documentos.
Alta velocidad para conversión masiva de documentos : 50, 90, 120, 300 páginas por minuto.
Fedatario supervisa que los documentos cumplen las normas técnicas de micrograbación.
Telefónica Servicios Digitales
Telefónica


Cómo Funciona: Ciclo de la Imagen
Indización
Se establece la identificación y los atributos para cada documento, para su posterior consulta y/o recuperación.
El Fedatario asegura que los datos corresponden a la imagen que hacen referencia.
Métodos
MANUAL (Vía Teclado)
OCR (Optical Character Recognition)
ICR (Intelligent Character Recognition)
OMR (Optical Marks Recognition)
IMR (Intelligent Magnetic Recognition)
BCR (Bar Code Recognition)
CARGO
ICR/OCR
Digitación
Telefónica Servicios Digitales
Telefónica

Cómo Funciona: Ciclo de la Imagen

Almacenamiento

- Un documento puede almacenarse en el disco magnético del servidor (Consulta Prioritaria)
- Puede ingresarse a sistema de segundo nivel = Jukebox (Consulta Necesaria)
- Se pueden archivar los discos ópticos en almacén para futuras consultas (Consulta Esporádica)
- Los medios de almacenamiento de las microformas se basan en la tecnología WORM
- Jukeboxes pueden contener millones de documentos

Discos Opticos



Jukeboxes/Autochangers

Telefónica Servicios Digitales

Telefónica

Cómo Funciona: Ciclo de la Imagen

Recuperación y Distribución

Visualización

Los documentos almacenados electrónicamente pueden ser consultados, impresos y transmitidos por cualquier medio compatible.

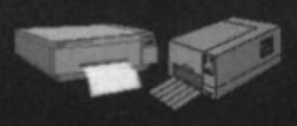


Internet / Intranet

- Visores corporativos
- Navegadores de Internet

Distribución:

Se utilizan impresoras láser, lo cual permite obtener copias identicas al original.



Impresoras, Transmisión Telemática

Telefónica Servicios Digitales

Telefónica

Beneficios

- Acceso a tecnología de punta sin necesidad de invertir
- Depreciación tecnológica a cargo del proveedor de servicios
- Pay per Use
- Acceso Concurrente a la información (redes de Telefónica, alcance nacional)
- Aplicación amplia de la tecnología gracias a las nuevas disposiciones legales

Telefónica Servicios Digitales

Telefónica

Antecedentes TSF

- 1996, nace Telefónica Servicios Financieros, filial de Telefónica del Perú. Como parte de sus soluciones integrales de Procesamiento de Medios de Pago se implementa la plataforma de digitación y digitalización para atender alrededor de 450,000 órdenes de pago al mes.
- Se amplió la plataforma de digitalización de altos volúmenes basada en una solución ' World Class'
- 1999, TSF obtiene el Certificado de Idoneidad Técnica emitido por Indecopi/SGS del Perú para darle valor legal a los medios digitales que genere.

Telefónica Servicios Digitales

Telefónica

Antecedentes COM S.A.

Empresa peruana de Consultoría, Tercerización de Servicios (Outsourcing) y Gerencia de Proyectos. Desde 1987 son líderes en la aplicación de tecnologías emergentes relacionadas al procesamiento de imágenes de documentos y en la prestación de servicios conexos.

- 2,500 millones de imágenes procesadas...
- RENIEC, FONAHPU, UNI, ORLC, ONPE, ONP, RPU, SEDAPAL principales Bancos, empresas del sector financiero y de seguridad social.

Telefónica Servicios Digitales

Telefónica



Telefónica Servicios Digitales

Telefónica



RESUMEN EJECUTIVO

Nombre: Richard Wadsworth Delgado
Profesión: Ingeniero de Sistemas

GERENCIA DE OPERACIONES TELEFÓNICA SERVICIOS FINANCIEROS S.A.C.

Compañía subsidiaria del Grupo Telefónica, ofreciendo servicios de procesamiento de datos orientados a la transacción y colocación de productos de valor agregado a los sectores financiero, de salud y de seguros, además de grandes retailers y corporaciones.

CLIENTES Y PROYECTOS :

- Servicio de procesamiento de datos a VisaNet, procesando transacciones de tarjetas VISA, Diners y en futuro próximo American Express, tanto en sus modalidades de crédito cómo de débito. Se procesa casi el 90% de las transacciones con tarjetas en el Perú. Instalación y Mantenimiento de terminales de punto de venta (POS) de la red de VisaNet a nivel nacional (aproximadamente 7,000 terminales).

- Cámara de Compensación Electrónica Interbancaria, orientada a manejar el canje de cheques, letras y otros instrumentos entre los miembros de nuestra comunidad financiera.

- Tarjeta de Servicios Integrados de Salud, orientado al las EPS y compañías de seguros y basado en la identificación de usuarios y autorización de atenciones.

- Autoridad de Registro representante de ACE (Agencia de Certificación Electrónica de España), para la comercialización y gestión de Certificados Electrónicos para el mundo de redes abiertas como Internet.

Tema 6

UNIVERSIDAD DERECHO E INFORMATICA

La Informática Jurídica aplicada en la Universidad Externado de Colombia

Dra. Teresa Vargas Osorno (Colombia)
Directora del Centro de Informática Jurídica Universidad Externado de Colombia

Cualquier actividad que se pretenda desarrollar con seriedad y eficiencia, requiere contar con la información pertinente en el momento adecuado. En la sociedad se evidencia tal necesidad en razón de la "explosión de información" que ha dado lugar a una "crisis en la información".

Es indudable que la modernización necesita generar cambios conceptuales que respondan a los nuevos esquemas mentales requeridos por el mundo moderno, lo cual implica mucho más que el simple hecho de instalar computadores u ordenadores. Se requiere una visión sistemática de los procesos de cambio y una voluntad férrea que dé continuidad y apoye el proceso.

El derecho no es ajeno al creciente volumen de información: cada vez es mayor el número de libros, revistas, leyes, códigos, fallos, etc. Que hacen imprescindible la utilización del computador para su archivo, procesamiento y utilización.

La complejidad y competitividad del mundo moderno hacen de la informática jurídica, la disciplina que le permite al profesional del derecho, soportar el cúmulo de información que diariamente se produce. No se puede desconocer entonces, la importancia que posee en la actualidad la informática jurídica, en las facultades de derecho. Es así como comparto la apreciación hecha por Joaquín Roig García: "Es evidente que el mundo del derecho no ha quedado al margen en esta rápida evolución y también se ha visto afectado por la implantación de la informática en la sociedad, no obstante, conviene destacar que para el derecho, la informática incide de dos maneras muy distintas, por una parte como herramienta de trabajo potencial con todo lo que dé mejora y progreso puede significar, y por otra como elemento al que hay que regular muy concienzudamente por su posibilidad de afectar de manera notable tanto a la esfera patrimonial como a la esfera personal de los ciudadanos".

Como instituciones formadoras de futuros juristas y profesionales del derecho en todos los campos, las facultades de derecho deben dar respuesta a estos dos aspectos mencionados, de un lado, dar a conocer a aquellos a quien acoge, las enormes posibilidades que como herramienta de trabajo ofrece la informática, y de otro lado formar a expertos en dicha materia, que contribuyan a que no se produzca un uso inadecuado"[1]

"El papel de las enseñanzas informáticas en los planes de estudio de las facultades de derecho, constituye un dato de relevancia incuestionable...". "Las repercusiones dela informática en el derecho están siendo cada vez más extensas en intensas. Dar cuenta de todas ellas resulta una tarea prácticamente inviable, entre otras cosas, por el carácter abierto y dinámico que reviste esa proyección. Baste pensar que, en el horizonte tecnológico del presente, muchos de los problemas y de las soluciones jurídicas tradicionales aparecen irremediablemente caducos. Ello impele a diseñar nuevos instrumentos de análisis y marcos conceptuales prontos para adaptarse a las exigencias de una sociedad en transformación. La informática jurídica y los sectores que la integran constituye una de las aportaciones con que cuenta la Teoría del Derecho actual para responder a esos apremios[2].

"La cibernética, puede ser considerada como la mayor novedad de la segunda mitad del siglo"[3] "La difusión de la información automatizada, que se pone ahora en primer plano del horizonte de la sociedad tecnológica a finales del siglo veinte, comporta una serie de consecuencias en el orden social, en el económico y en el jurídico"[4].

---

[1] ROIG GARCIA, Joaquín; Aulas de Informática y Facultades de Derecho. Aproximación a un desarrollo práctico. Informática y Derecho. Págs.699-705.

[2] PEREZ LUÑO, Antonio Enrique. La Informática Jurídica en la Investigación y Enseñanza del Derecho. Informática y Derecho, págs. 55-70.

[3] FROSINI. Contributi ad un diritto dell'informazione, págs. 211-212

[4] FROSINI. Contributi ad un diritto dell'informatzione, pág. 159

Esa novedad de la segunda mitad del siglo, novedad de la cibernética afecta a las universidades, a las tareas de investigación y de enseñanza. Así como también presenta consecuencias en el orden académico: el computador está incidiendo en los ámbitos de la investigación y de la enseñanza. Análogamente a como la máquina de escribir fue superada por el procesador de palabras y la copia con papel carbón fue sustituida por la impresora aneja al computador o por la fotocopiadora, atrás quedó la penosa consulta manual de una información dispersa. De aquí en adelante comienza una fascinante historia que desemboca en "la actual escritura binaria de las computadoras"[5].

El computador es una herramienta eficaz, un instrumento en la mano del hombre, que le permiten un mejor desarrollo dentro de la sociedad. Las faculades de derecho deben estar conscientes, y lo están cada vez más, de la necesidad de asumir el reto de incorporar en su seno aulas de informática jurídica aplicada, que forme futuros juristas en este campo. Hay que reconocer que con la informática jurídica al profesional del derecho se le abren nuevos caminos en el desarrollo de sus actividades.

En mi opinión la enseñanza de la informática jurídica en las facultades de derecho debe ir más allá de las aplicaciones prácticas; debe haber un conocimiento profundo tanto de la informática jurídica como del derecho informático.

En cumplimiento de su deber de mantenerse actualizada e ir a la vanguardia académica, la UNIVERSIDAD EXTERNADO DE COLOMBIA, merced a un trabajo inmenso y esmerado, incorpora al patrimonio cultural de la profesión jurídica la técnica y la metodología más avanzadas, orgullosa de ser pionera en el ofrecimiento de los bancos de datos jurisprudenciales. Abogados, litigantes, jueces, fiscales, magistrados, empresas, instituciones, asesores, alumnos, profesores, investigadores, académicos e intelectuales podrán acceder al volumen íntegro y actualizado de la doctrina de las altas Cortes en el disco compacto. Atrás quedó la penosa consulta manual de la jurisprudencia, ahora la podremos encontrar articulada y clasificada.

Es muy satisfactorio para la Universidad Externado de Colombia - Departamento de Informática Jurídica, presentar al público de estudiosos del derecho los tres primeros ejemplares de la colección de bancos de datos jurídicos. El primer ejemplar es el de "CONTRATACION ESTATAL", que es una recopilación completa de legislación concordada y providencias de la Corte Constitucional y del Consejo de Estado desde 1983 hasta la fecha, cuidadosamente analizadas y clasificadas de acuerdo con la metodología jurídica y el tesauros.

El segundo ejemplar es el de "JURISPRUDENCIA PENAL", integrado por las principales providencias proferidas por la Sala de Casación Penal de la Corte Suprema de Justicia, en las que se plantean y solucionan los distintos problemas jurídicos que giran alrededor del desarrollo y perfeccionamiento teórico práctico del derecho penal en general, como mecanismo de control social formal que integra el sistema penal.

El tercer ejemplar es el de "JURISPRUDENCIA LABORAL", integrado por las providencias proferidas por la Sala de Casación Laboral de la Corte Suprema de Justicia, en las que se plantean y solucionan los distintos problemas jurídicos que giran alrededor del desarrollo y perfeccionamiento teórico-práctico del derecho laboral.

Posteriormente se editarán los bancos de datos de jurisprudencia de la Corte Constitucional, Corte Suprema de Justicia Sala de Casación Civil, jurisprudencia en derecho de familia y legislación y jurisprudencia de derecho de seguros.

COMO CONSTRUIMOS NUESTRAS BASES DE DATOS

En la elaboración de dichos Bancos de Datos se resaltan como puntos principales el desarrollo de TESAURUS JURIDICOS para cada una de las áreas, la metodología jurídica para el análisis de la jurisprudencia (problema jurídico, tesis, fuente formal, descriptores y texto completo en el banco de datos de contratación estatal y extracto en los demás bancos). En los bancos de datos en que se toma sólo el extracto no se incluyen todos los fallos, sólo

[5] EUGENIO, Francisco. Informatización del Derecho. Universidad, Computación y Derecho: sobre sus implicaciones recíprocas. Informática y Derecho. Pág. 72

aquellos que den lugar a extracto jurisprudencial después del correspondiente análisis; pues hay sentencias y autos que no merecen ser incorporados a la base de datos en razón a que la Corte no siente ningún tipo de doctrina sino que se limita al análisis de pruebas. En el banco de datos de Contratación Estatal se incluye el texto completo y todas las providencias emitidas por la Sección Tercera del Consejo de Estado y de la Sala de Consulta y Servicio Civil que tengan que ver con el tema de Contratación Estatal.

Dentro de nuestro análisis de providencias judiciales señalamos:

1º. Datos que identifican el documento: Tales como el autor, sea corporativo o personal, título de la providencia que indica la fecha de la misma, nombre del Magistrado o Consejero Ponente, demandante, demandado, expediente, notas en donde se incluyen las sentencias y autos en igual sentido y en sentido contrario que ha señalado la misma providencia que se analiza.

2º. Análisis: Al estar frente a una providencia nos planteamos el problema o problemas jurídicos a los cuales la Corporación les está dando respuesta. A cada problema jurídico se le extrae la respuesta que constituye la tesis que se incorpora a la base de datos. Esta tesis es textual.

También a cada problema jurídico se le señala su correspondiente texto para el banco de datos de contratación estatal y extracto jurisprudencial para los demás bancos, que es donde la Corporación fundamenta ese problema, sentando doctrina, lo cual se transcribe.

Al problema jurídico se le asigna la fuente jurídica que la Corporación tuvo en cuenta para darle solución al mismo.

Todo esto se titula con un descriptor o varios sacados de los tesauros jurídicos debidamente elaborados en cada área por el departamento.

COMO CONSULTAMOS LAS BASES DE DATOS

Se hizo lo posible para que la búsqueda fuera sencilla y para que el usuario tenga la posibilidad de hacer distintas combinaciones de búsqueda sin tener un conocimiento profundo sobre computadores. Se utiliza el manejador de archivos MICRO CDS/ISIS, distribuido por COLCIENCIAS-ACOFI, para registrar los datos identificadores de cada una de las providencias que van al Banco de Datos. Se utiliza el procesador de textos para la grabación de los textos y extractos jurisprudenciales. La Universidad desarrolló un programa interfase que hace amigable la consulta y permite la unión de lo grabado en ISIS con el texto o extracto grabado en el procesador de palabra, es así como el usuario final puede consultar los bancos de datos en un CD ROM.

En este orden de ideas, las opciones para consulta de cada una de las bases de datos son:

1. POR TEMA: Por los descriptores asignados de acuerdo al tesauros elaborado para cada área.

2. POR TITULO: El cual está conformado por la denominación de la providencia (sentencia, auto, salvamento de voto, etc.) y la fecha.

3. POR FECHA: Fecha de la providencia.

4. POR AUTOR PERSONAL: Permite la consulta de los salvamentos y aclaraciones de voto hechos por un magistrado.

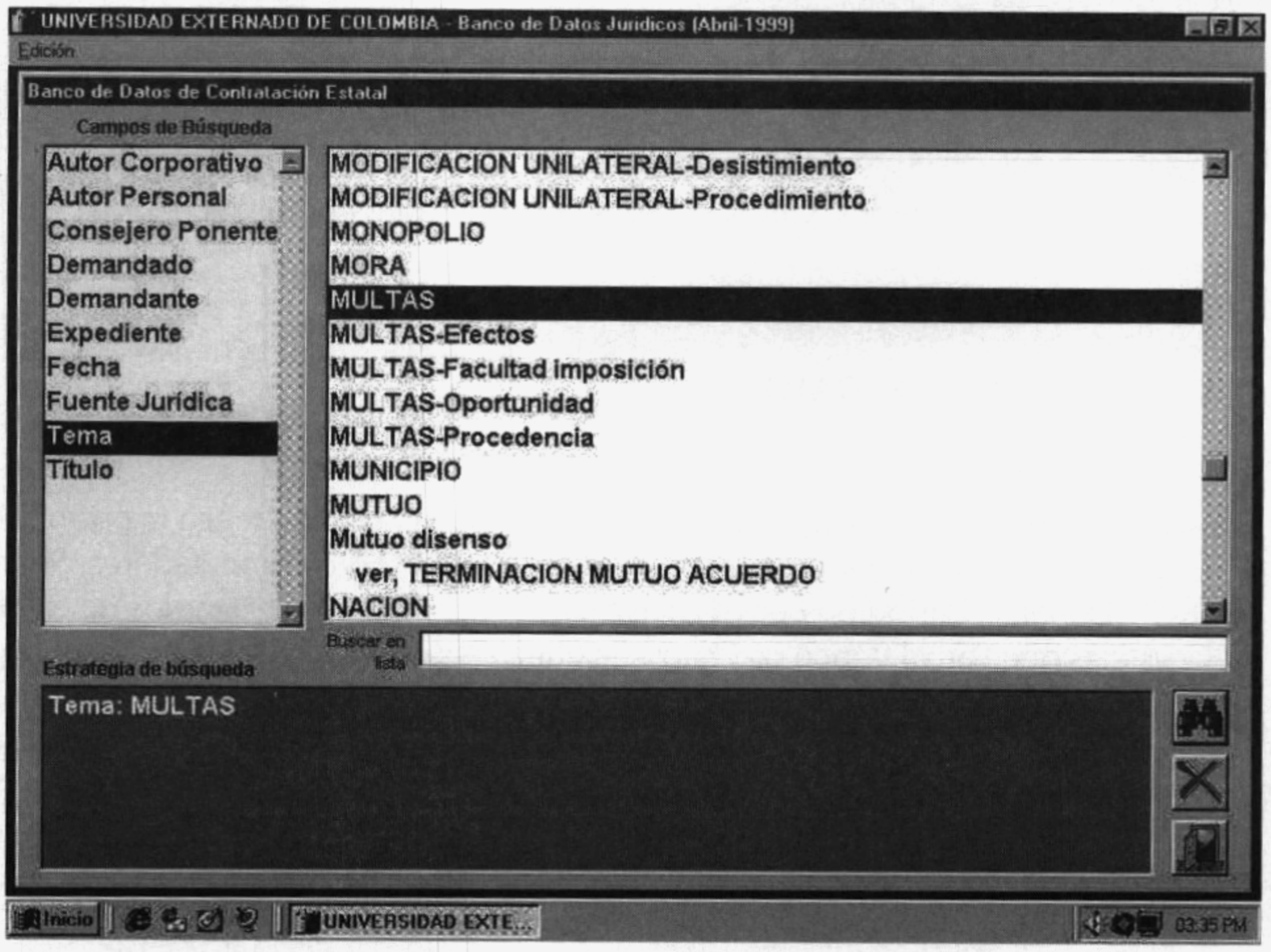
5. POR MAGISTRADO: Indice que contiene los nombres de los magistrados de la respectiva Sala.

6. POR FUENTE FORMAL: Indice que contiene las fuentes jurídicas que sustentan cada una de las tesis de la Corporación en sus respectivas áreas.
7. POR DEMANDANTE: Indice que contiene el listado de demandantes.
8. POR DEMANDADO: Indice que contiene el listado de demandados.
9. POR EXPEDIENTE: Indice que contiene el número de radicación de las providencias.

La consulta puede realizarse independientemente por cada uno de los campos señalados anteriormente o mediante la combinación con los conectores lógicos Y u O. El usuario tiene la opción de ver e imprimir lo consultado que consta de los datos identificadores de la providencia, tesis y texto (para el banco de datos de contratación estatal) o extracto jurisprudencial (para los demás bancos de datos). Además puede enviar a su procesador de palabra lo que desee después de hacer la consulta, como también buscar palabras dentro del texto. Los bancos de datos que se manejan con extracto jurisprudencial, si el usuario desea obtener el texto completo de la providencia lo encuentra en los archivos del departamento.

A continuación mostraremos un ejemplo con las bases de datos de Contratación Estatal y Jurisprudencia Penal:

Usted encuentra una primera pantalla dividida en varios cuadros:



Un primer campo cuadro llamado "campos de búsqueda" que muestra los siguientes elementos de búsqueda: Autor corporativo, autor personal, consejero ponente, demandado, demandante, expediente, fecha fuente jurídica, tema y título.

Un segundo cuadro llamado "cuadro índice de información" que muestra la lista de los elementos en orden alfabético.

Un tercer cuadro llamado "estrategia de búsqueda" en donde aparecen los elementos seleccionados para la búsqueda.

Para escoger el campo de búsqueda en la casilla campos para buscar desplace la barra hasta el lugar deseado moviendo el puntero del mouse y pulse una vez; por ejemplo: Tema.

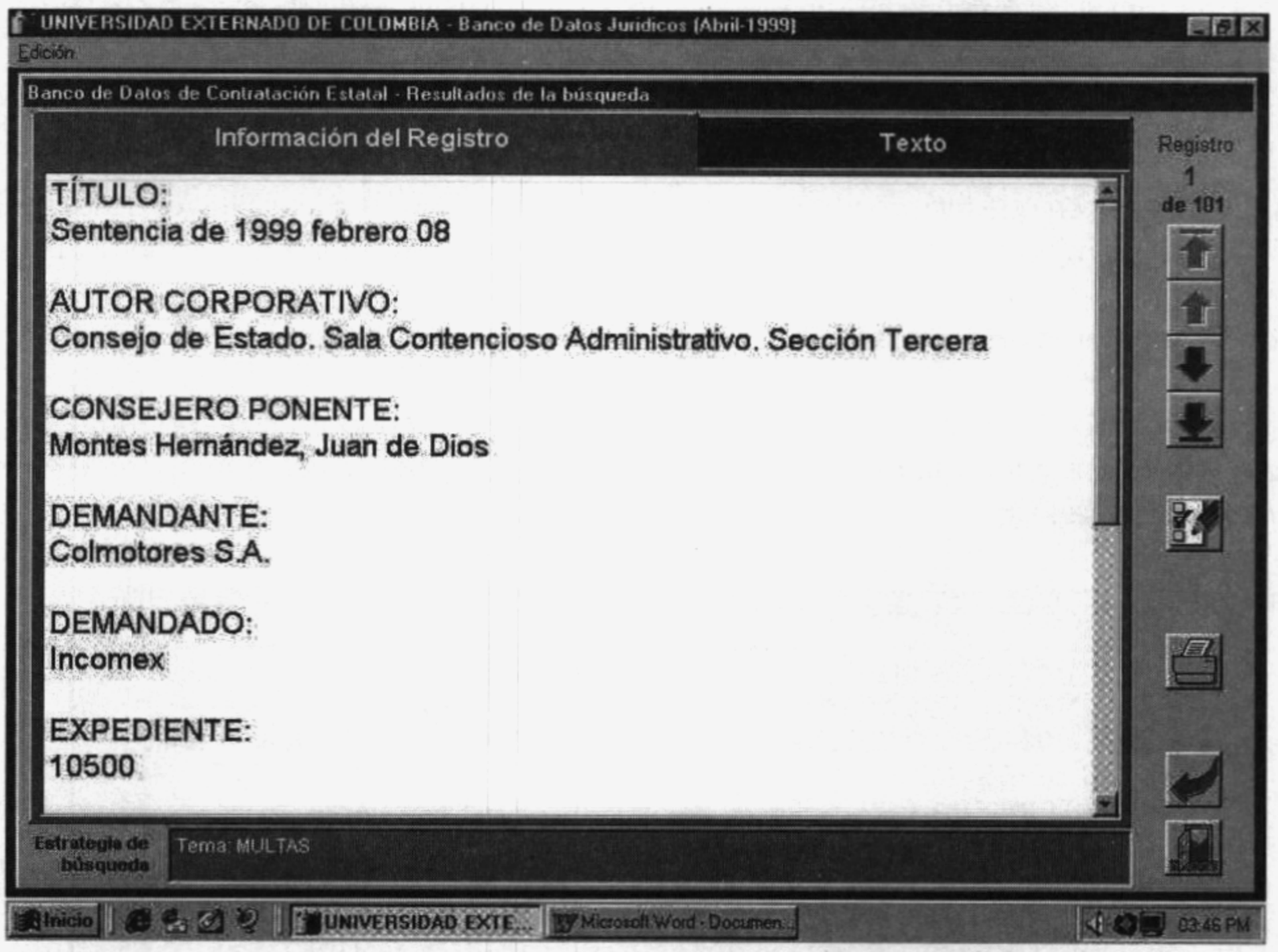
Al escoger el campo de búsqueda en la casilla índice de la información aparece la lista de los elementos correspondientes en orden alfabético. Para desplazarse dentro de esta casilla se puede llevar el puntero del mouse al lugar deseado y pulsar una vez; utilizar las flechas de la barra de desplazamiento vertical; utilizar las flechas del teclado u oprimir la letra inicial del elemento que desee buscar; ejemplo: A, S, T,. Si se conoce el nombre del elemento que intenta buscar, por ejemplo MULTAS, escríbalo en la casilla "buscar en lista" y pulsar Enter.

Si desea seleccionar un elemento se debe llevar el puntero del mouse al lugar deseado y pulsar dos veces o pulsar Enter.

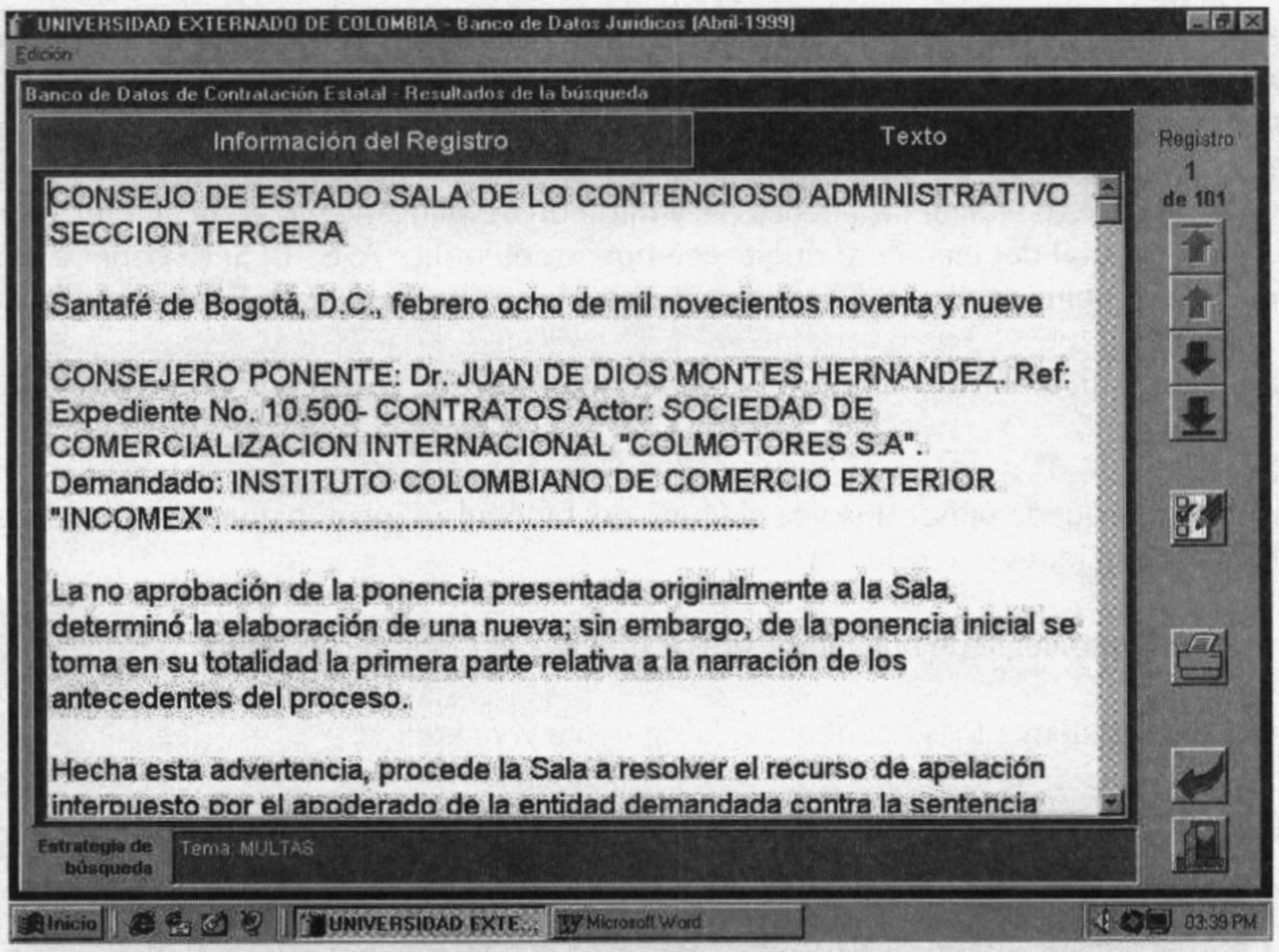
Para comenzar la búsqueda pulsar una vez el ícono del binóculo. Con ello aparecerá en el cuadro "estrategia de búsqueda" la o las selecciones que usted hizo.

Si desea cancelar la estrategia de búsqueda, pulsar una vez el ícono de "cancelar búsqueda".

Seleccionado el o los elementos encontramos la siguiente ventana:



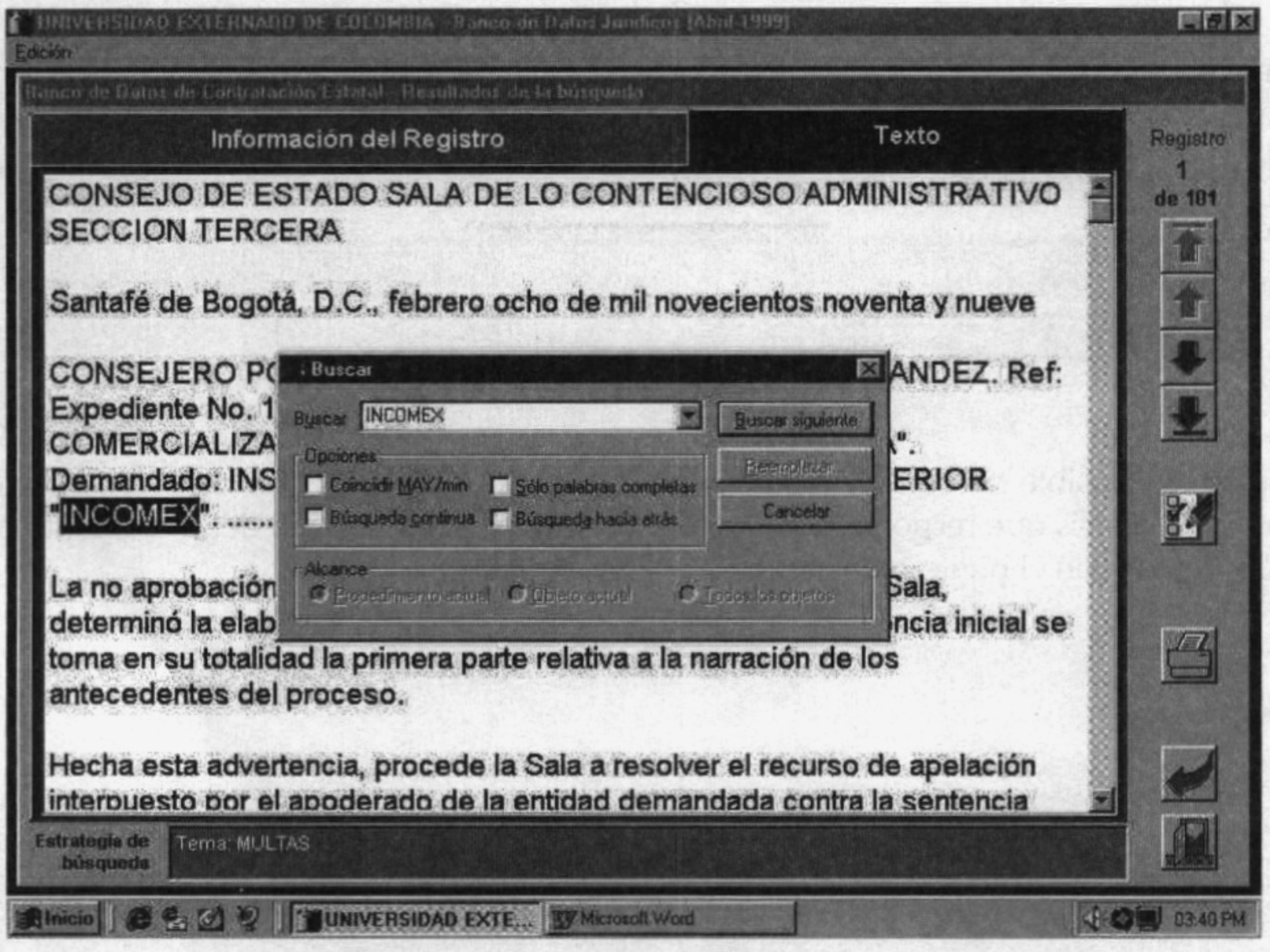
En esta ventana es posible consultar los datos que identifican el registro con la clase de documento (legislación o providencia), y la tesis que responde a un problema jurídico; e ir al texto del documento mismo pulsando una vez la opción "texto" con el puntero del mouse.



La pantalla nos muestra en qué registro nos encontramos ubicados y nos permite a través de las flechas desplazarnos de un registro a otro. En el ejemplo de MULTAS tenemos 101 registro y estamos situados en el primer registro.

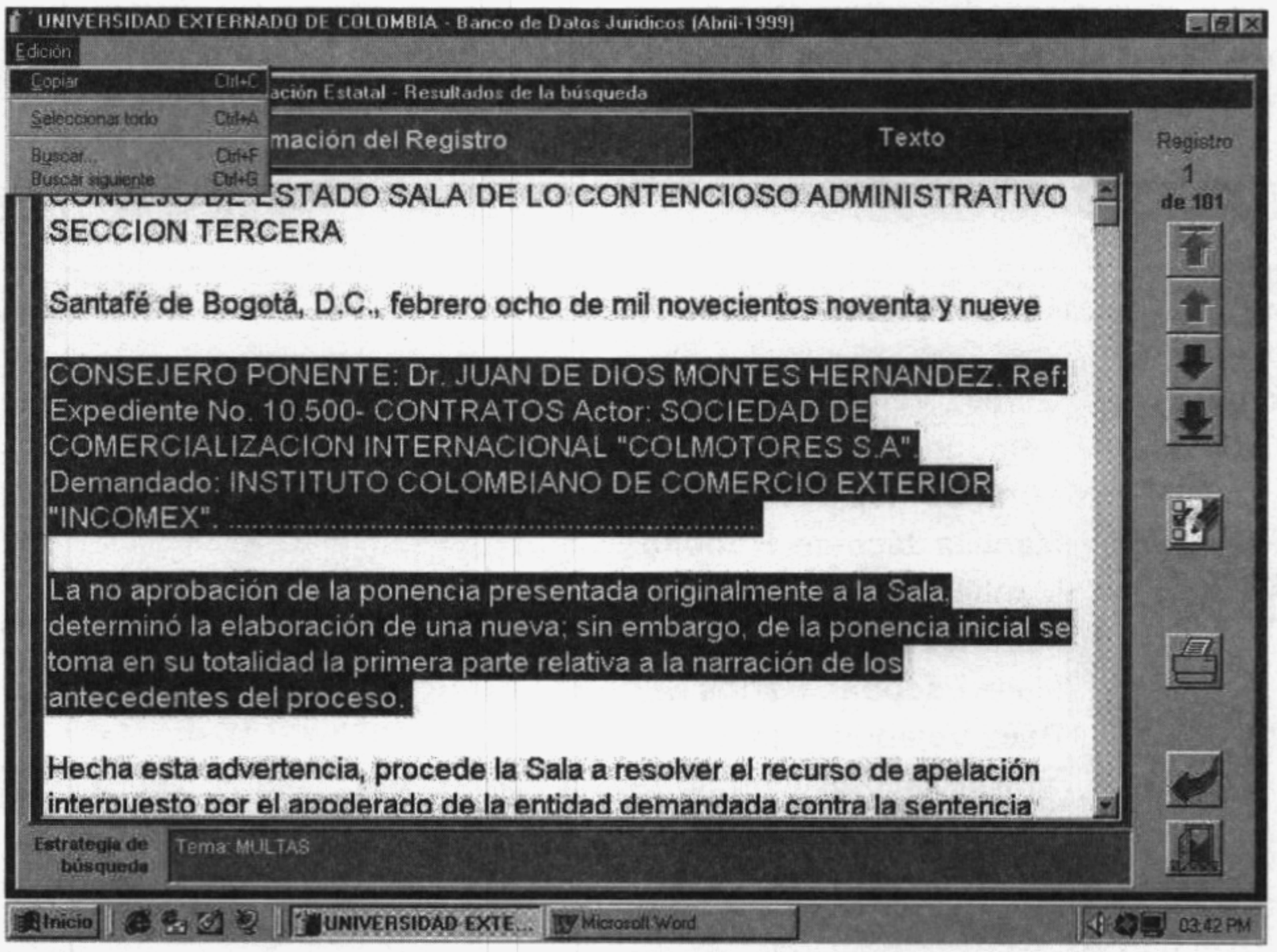
Hay funciones de edición en cuya opción se encuentran las siguientes funciones:

BUSCAR: En el cuadro "buscar" se escribe el texto que se desea encontrar. A continuación, pulsar el botón buscar siguiente o Enter para iniciar la búsqueda y para buscar la siguiente vez que aparèce el texto en el documento pulsar buscar siguiente.



COPIAR: Nos permite llevar a un procesador de palabra el texto o parte de él. Se debe seleccionar el texto que se desea copiar e ir a edición y pulsar copiar. Si usted se encuentra en otra aplicación, cierre la ventana y abra el documento o la aplicación deseada y en la opción edición pulse pegar.

SELECCIONAR TODO: Nos permite seleccionar todo el texto.

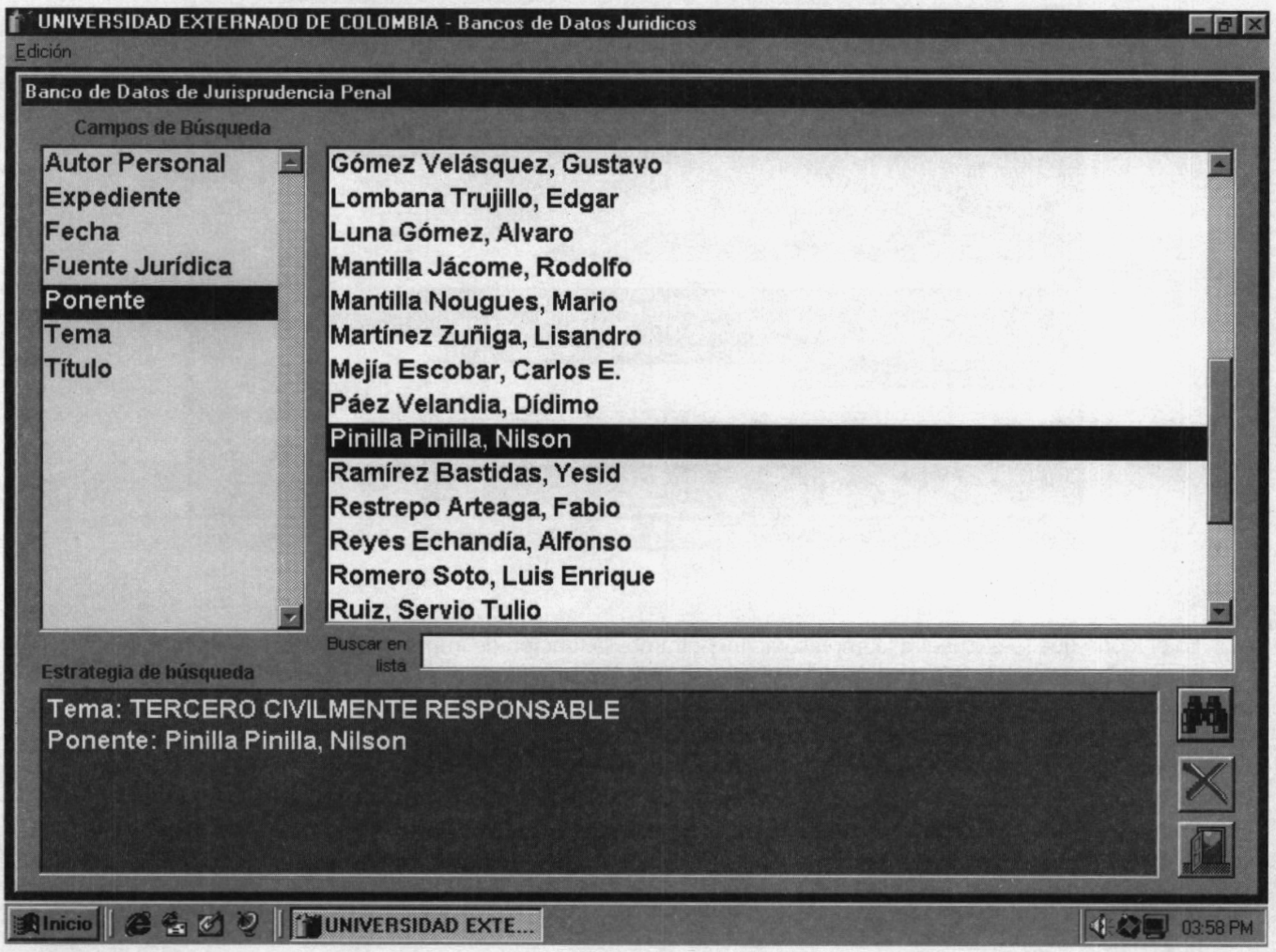


En el ícono que se encuentra la impresora, encontramos la función de impresión que permite: Imprimir la información del registro, imprimir la información del registro y su texto, imprimir todos o sólo los registros seleccionados.

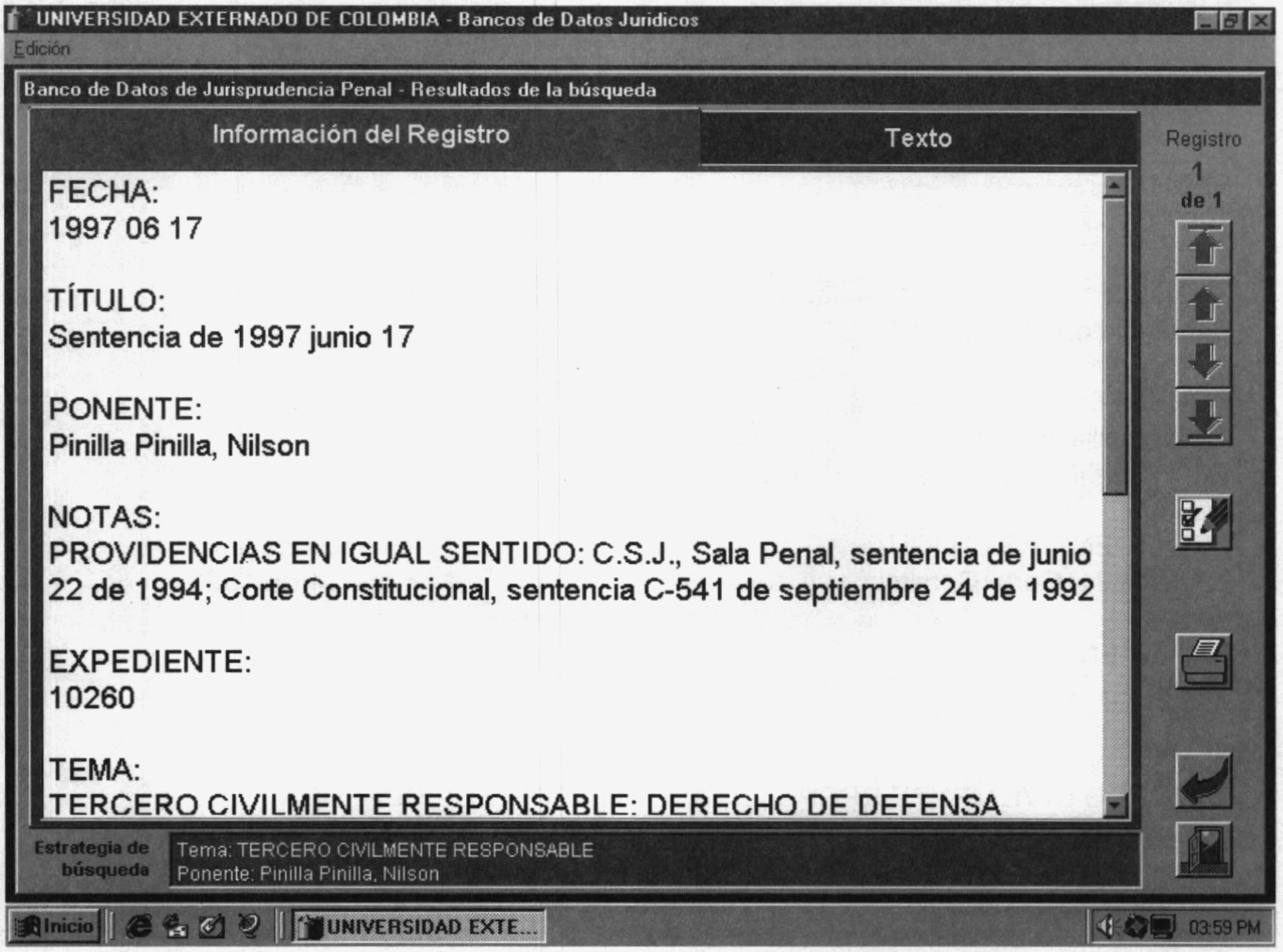
A continuación procederemos a mostrar un ejemplo que explica la forma igualmente sencilla y fácil como se puede consultar la información contenida en el Banco de Datos de Jurisprudencia Penal.

En materia penal existe actualmente toda una discusión que gira alrededor de la figura del tercero civilmente responsable, debido a que el estatuto procesal que nos rige no reguló integralmente dicha figura, omitiendo aspectos tan importantes como la oportunidad procesal con que se cuenta para lograr su vinculación.

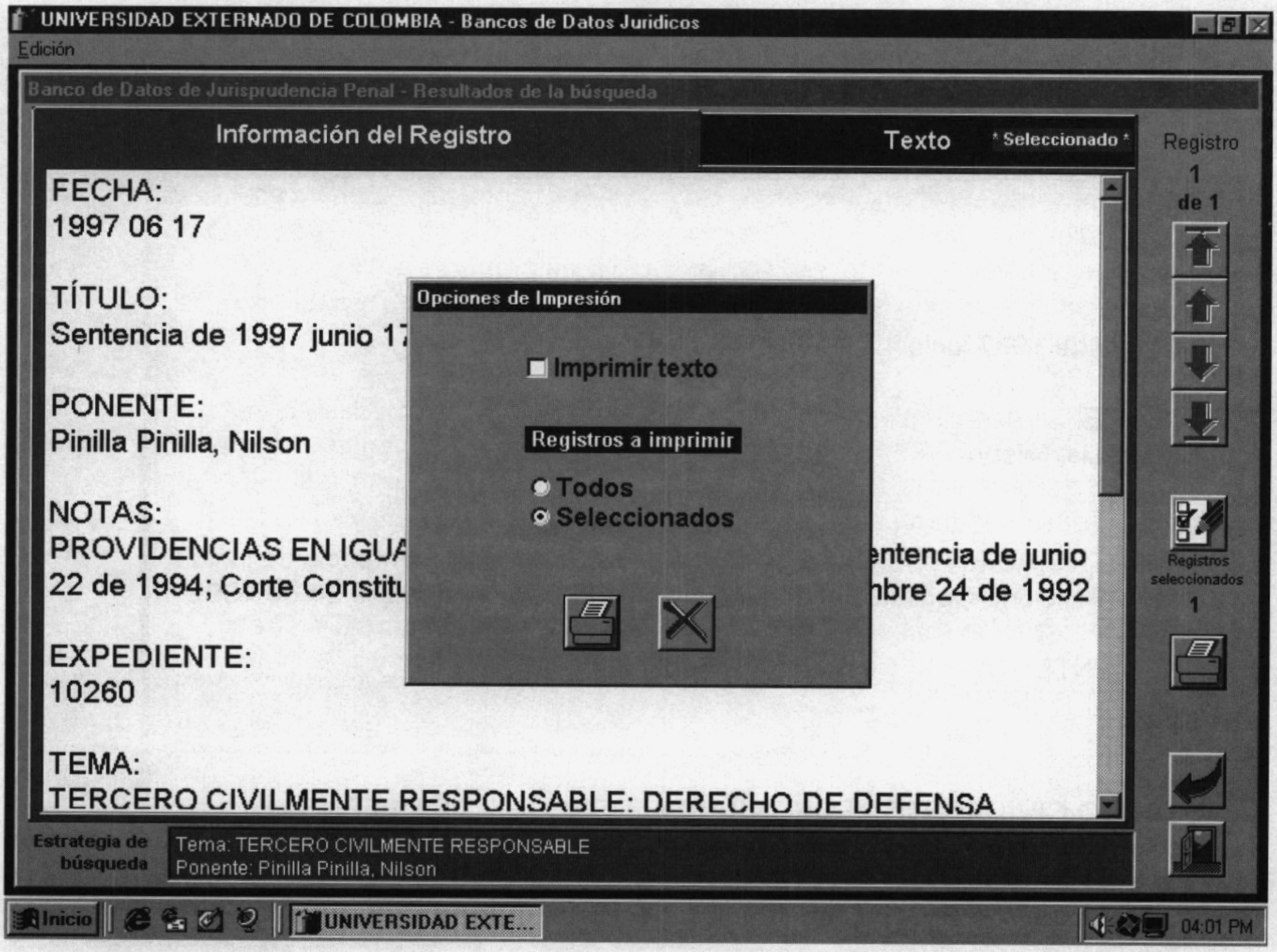
Pues bien, si nosotros queremos saber cual es la posición que frente a este importante tema tiene la Sala de Casación Penal de la Corte Suprema de Justicia, podemos consultar nuestro banco de datos ubicándonos en la pantalla inicial de búsqueda y seleccionando en el campo de "temas" el descriptor TERCERO CIVILMENTE RESPONSABLE, en la forma como se explicó cuando se dio el ejemplo en contratación estatal. Pero si nosotros adicionalmente queremos saber en concreto que ha dicho sobre la figura del tercero civilmente responsable el magistrado Nilson Pinilla Pinilla, podemos combinar los campos de búsqueda, seleccionando simultáneamente por ponente, en la pantalla inicial de búsqueda, a dicho magistrado. Apareciendo en la pantalla "estrategia de búsqueda" los campos correspondientes al "tema": TERCERO CIVILMENTE RESPONSABLE y "ponente": Pinilla Pinilla, Nilson., como se muestra en la siguiente gráfica:

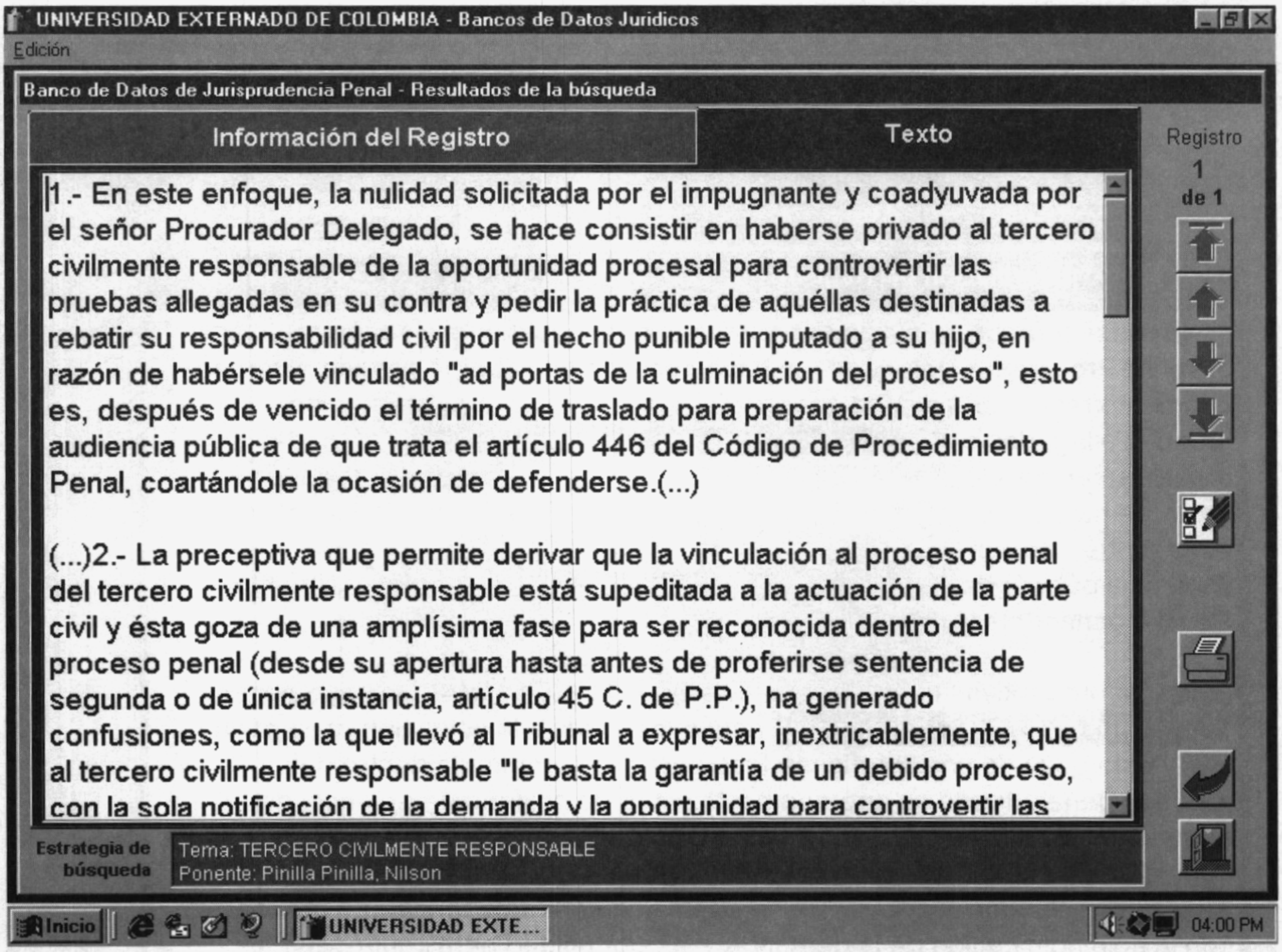


A continuación nos ubicamos con el mouse en el botón donde aparece el binocular y hacemos clik, para que inicie la búsqueda y nos muestre la información consultada, contenida en el registro (fecha, título, ponente, notas, expediente, tema, tesis y fuente jurídica), tal como se observa en la siguiente gráfica:

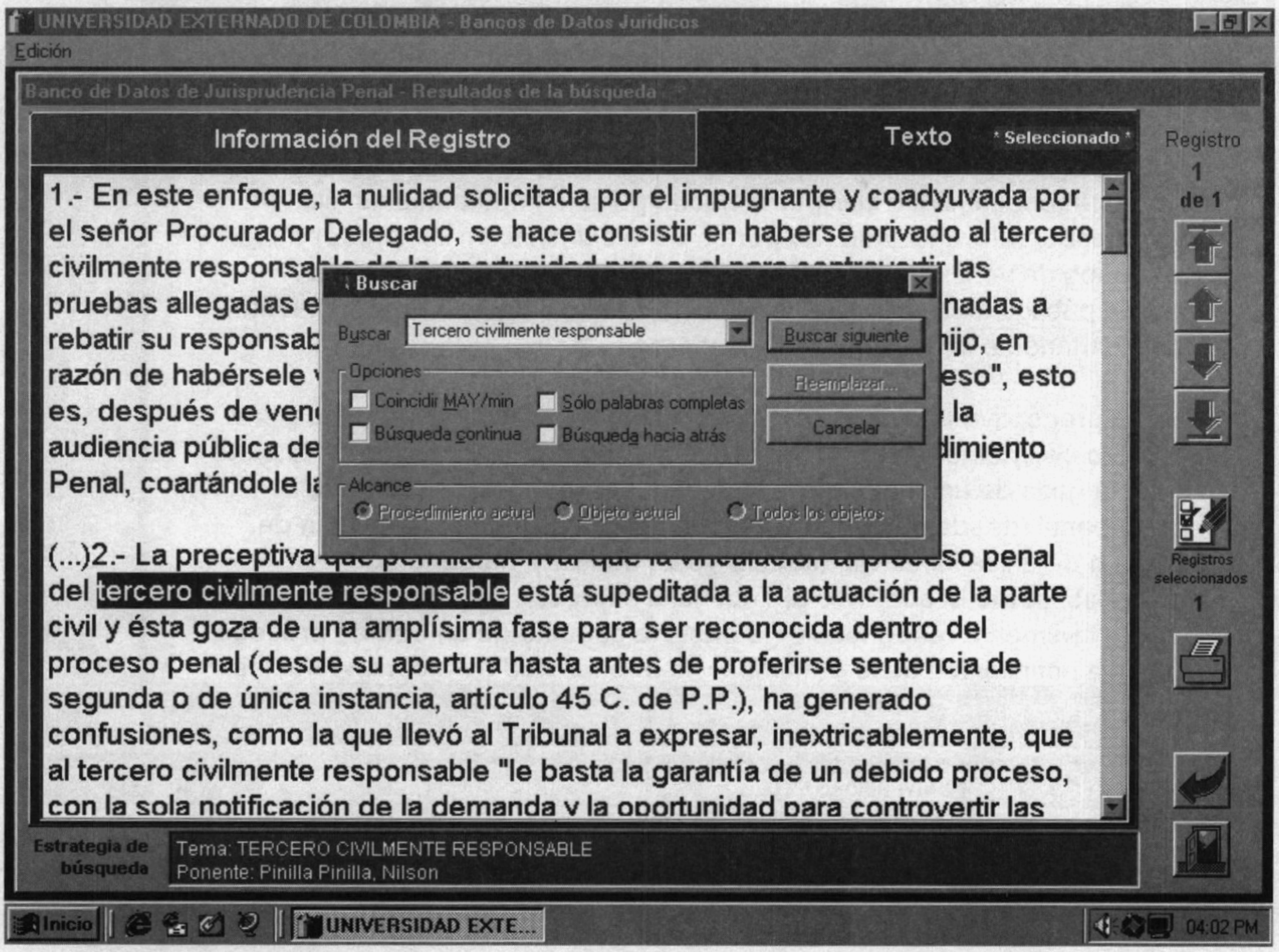


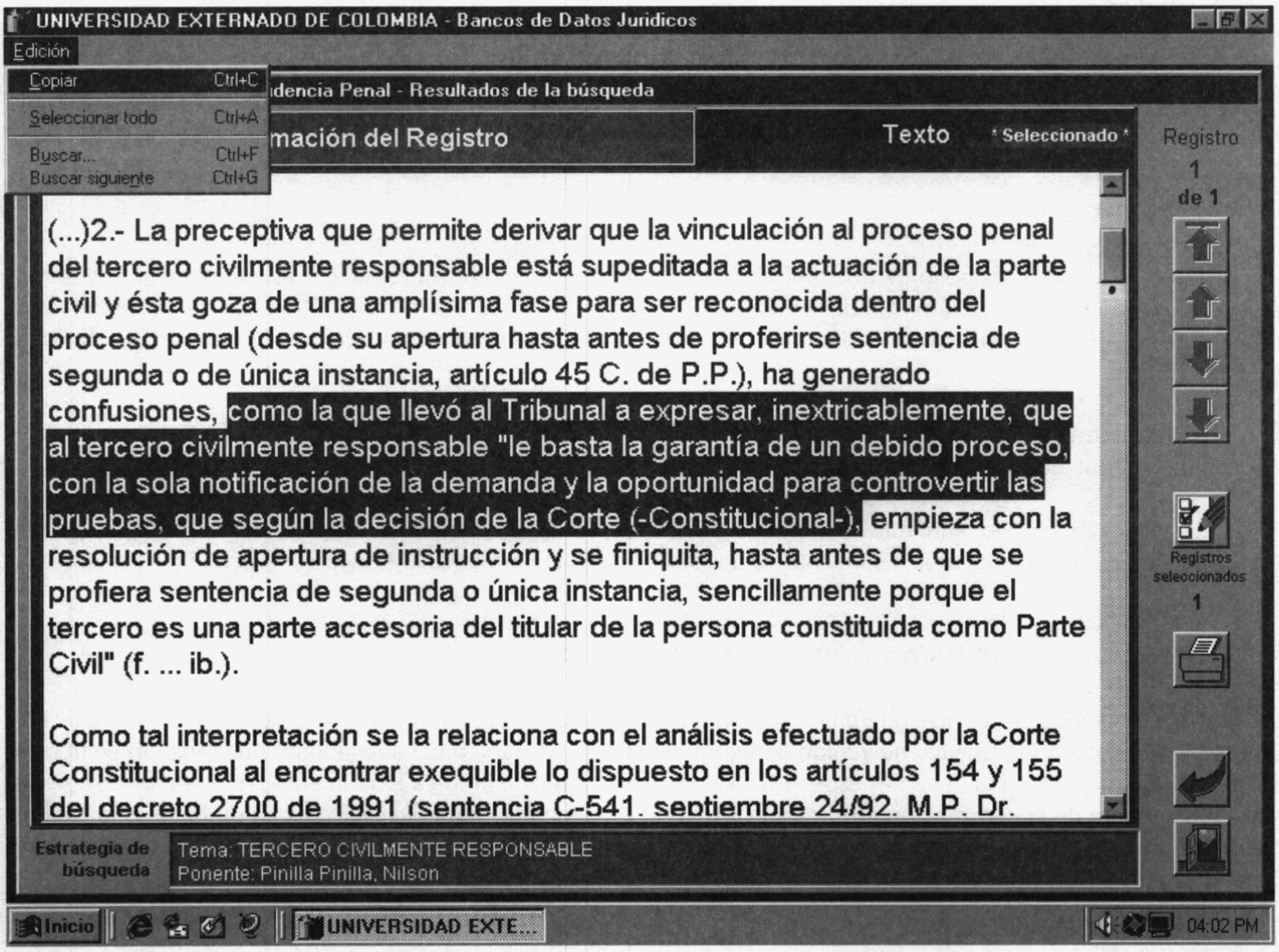
Si queremos indagar por el extracto de la providencia, lo podemos hacer con la opción de consulta "texto" e inmediatamente el programa nos muestra dicho extracto, tal como se aprecia en la gráfica:




UNIVERSIDAD EXTERNADO DE COLOMBIA - Bancos de Datos Juridicos
Edición
Banco de Datos de Jurisprudencia Penal - Resultados de la búsqueda
Información del Registro
Texto
Registro
1
de 1
1.- En este enfoque, la nulidad solicitada por el impugnante y coadyuvada por el señor Procurador Delegado, se hace consistir en haberse privado al tercero civilmente responsable de la oportunidad procesal para controvertir las pruebas allegadas en su contra y pedir la práctica de aquéllas destinadas a rebatir su responsabilidad civil por el hecho punible imputado a su hijo, en razón de habérsele vinculado "ad portas de la culminación del proceso", esto es, después de vencido el término de traslado para preparación de la audiencia pública de que trata el artículo 446 del Código de Procedimiento Penal, coartándole la ocasión de defenderse.(...)
(...)2.- La preceptiva que permite derivar que la vinculación al proceso penal del tercero civilmente responsable está supeditada a la actuación de la parte civil y ésta goza de una amplísima fase para ser reconocida dentro del proceso penal (desde su apertura hasta antes de proferirse sentencia de segunda o de única instancia, artículo 45 C. de P.P.), ha generado confusiones, como la que llevó al Tribunal a expresar, inextricablemente, que al tercero civilmente responsable "le basta la garantía de un debido proceso, con la sola notificación de la demanda y la oportunidad para controvertir las
Estrategia de búsqueda
Tema: TERCERO CIVILMENTE RESPONSABLE
Ponente: Pinilla Pinilla, Nilson
Inicio
UNIVERSIDAD EXTE...
04:00 PM

Al igual a como se explicó para la consulta de contratación estatal, esta base de datos cuenta con la función de impresión y las funciones de edición, buscar, copiar y seleccionar todo. Ver las gráficas que se muestran a continuación:




UNIVERSIDAD EXTERNADO DE COLOMBIA - Bancos de Datos Juridicos
Edición
Copiar Ctrl+C
Seleccionar todo Ctrl+A
Buscar... Ctrl+F
Buscar siguiente Ctrl+G
idencia Penal - Resultados de la búsqueda
mación del Registro
Texto
* Seleccionado *
Registro
1
de 1
(...)2.- La preceptiva que permite derivar que la vinculación al proceso penal del tercero civilmente responsable está supeditada a la actuación de la parte civil y ésta goza de una amplísima fase para ser reconocida dentro del proceso penal (desde su apertura hasta antes de proferirse sentencia de segunda o de única instancia, artículo 45 C. de P.P.), ha generado confusiones, como la que llevó al Tribunal a expresar, inextricablemente, que al tercero civilmente responsable "le basta la garantía de un debido proceso, con la sola notificación de la demanda y la oportunidad para controvertir las pruebas, que según la decisión de la Corte (-Constitucional-), empieza con la resolución de apertura de instrucción y se finiquita, hasta antes de que se profiera sentencia de segunda o única instancia, sencillamente porque el tercero es una parte accesoria del titular de la persona constituida como Parte Civil" (f. ... ib.).
Como tal interpretación se la relaciona con el análisis efectuado por la Corte Constitucional al encontrar exequible lo dispuesto en los artículos 154 y 155 del decreto 2700 de 1991 (sentencia C-541, septiembre 24/92. M.P. Dr.
Registros seleccionados
1
Estrategia de búsqueda
Tema: TERCERO CIVILMENTE RESPONSABLE
Ponente: Pinilla Pinilla, Nilson
Inicio
UNIVERSIDAD EXTE...
04:02 PM

3.1.- ¿Para que enseñar?

La primera cuestión que debemos respondernos es ¿para que vamos a enseñar informática a los abogados?. La respuesta permitirá tener claras las metas y a su ves posibilitara una clara explicación a los alumnos de dicho porque.

A mas de todas las razones expuestas, facilidad, celeridad y seguridad entre otros beneficios que brinda la informática al graduado en derecho no podemos dejar de decir que quien no posee un grado de conocimiento mínimo en la materia será un futuro analfabeto, este ítem no tiene argumento serio en contra[3], si queremos profesionales de primera línea deben "saber" informática.

3.2.- ¿Que enseñar?

Esta segunda pregunta requiere una respuesta más compleja que la anterior porque implica determinar y compatibilizar contenidos en forma vertical y horizontal a fin de fijar el perfil del graduado.

Hay experiencias de diversos tipos, aquellos que solo dictan clases de determinados programas que se suponen mas útiles que otros en una elección al azar, quienes han pretendido convertir a los abogados en analistas de sistemas por solo mencionar los dos ejemplos más claros.

Por nuestra parte entendemos al futuro profesional se lo debe capacitar con los conocimientos necesarias que le permitan usar y comprender el funcionamiento del hardware y del software de un determinado momento, pero también debe brindársele el grupo de conocimientos necesarios que le permita "migrar" de equipo o de software sin grandes problemas. Esto último asegura un profesional que tenga la capacidad de estar siempre en lo último, de usar siempre lo mejor, si no logramos este segundo objetivo tenemos a un alumno, graduado o profesional paralizado en el tiempo.

Para lograr esto es necesario al menos impartir el siguiente grupo de conocimientos:

a) Estructura de Computadoras:

- De hardware, diversos tipos de dispositivos, marcas, velocidades, placas, sistemas, unidades de medida, compatibilidad entre fabricantes, terminología, etc.

- De software, Sistemas Operativos, tipos de software, unidades lógicas, comandos y funciones comunes, compatibilidades, marcas, IGU, estructura de árbol, directorios, carpetas, archivos, etc.

b) Uso de Sistemas Operativos: esto implica el uso de los comandos y herramientas básicas del sistema operativo que se decida utilizar. Elegir el sistema operativo sobre el cual se trabajara es una cuestión de oportunidad, hoy, por mucho que nos duela debemos trabajar sobre las plataformas de Microsoft, pues es lo que el mercado exige y tiene. Quizás sea preferible trabajar sobre un mejor sistema, o sobre uno libre de derechos (Linux), pero que objeto tiene, si lo que formamos son abogados (perfil general del egresado que nunca debe perderse de vista).

c) Procesadores de Textos: tanto para el estudiante como para el abogado el procesador de textos es el programa con el que tendrán que convivir. Esta herramienta es imprescindible, todo graduado en derecho debe manejar a la perfección al menos un procesador de textos, ello implica la posibilidad de usar sus comandos comunes (negritas, sangría, letras, etc.), los avanzados (márgenes, corrección automática, etc.) y por supuesto implica poder mudarse de tipo y numero de programa (vgr. Pasar del Word al WordPerfect, etc.)

[3] Solo baste como ejemplo mencionar que el trabajo calificado requiere conocimiento de PC tal como hace 40 años exigía tener la doble escolaridad terminada y como hace 70 años se exigía saber leer y escribir.

La importancia del uso del procesador de texto solo alcanza a ser comprendida por el estudiante cuando nosotros como docentes logramos transmitir las ventajas competitivas que tendrá (conociendo la herramienta) frente a quien posea instrucción en el uso.

d) Utilidades: implica el uso de manejadores de archivos especializados (Norton, WinCommander), el uso de antivirus, compactadores, grabadores, etc.

e) Planilla de Calculo: solo en lo mínimo necesario para control de gastos y algunas opciones de gráficos. Si se dispone de tiempo sería muy recomendable avanzar sobre otros aspectos más avanzados.

f) Programas de uso jurídico especifico: implica programa de recupero de información que normalmente se encuentra en CD. El recupero de información tiene un lógica especial de búsqueda, hay que saber usar los operadores booleanos que acortar el fichero y ganan tiempo.

También existen programa para gestionar estudios y juzgados, tales como Advocatus o Lex-Doctor, el dictado de estos programas es muy útil para el graduado porque le facilitan las tareas profesionales.

Si se dispone de tiempo los programas de bases de datos generales pueden ser de mucho provecho.

g) Internet:

- Teoría: un buen uso de Internet no puede hacerse si no se tiene conocimiento acerca del funcionamiento de la misma, y sobre cual es el origen histórico de la red. Necesariamente debn impartirse los conceptos de protocolo, criptografía, enlaces, siglas, orígenes, etc.

- Web y Navegadores : la web es el servicio estrella de la net, su uso es clave para obtener información. El conocimiento de un navegador permite acortar paginas y ahorrar tiempo (favoritos, atajos, etc). Dentro del servicio web no puede dejarse de enseñar acerca del uso de los buscadores, esto se verá facilitado porque en líneas generales se usan operadores de búsqueda similares a los usados en programas de recupero de información[4].

- E-mail: a través de webmail o de cuentas POP3. El uso del servicio de mail es clave para el intercambio de información, sin dejar de mencionar que en un futuro cercano las consultas de expedientes y el envió de información podrán (y hasta deberán) hacerse vía módem.[5]

- IRC: el uso del IRC no solo permite el esparcimiento y el uso lúdico de las computadoras sino que también permite la teleconferencia (aunque en una forma muy primitiva) pero adapta para una nueva forma de intercambio de información.

Nosotros creemos que este plan expositivo no debe alterarse, al menos no en su esencia, así por ejemplo no podría enseñarse Internet, antes de los procesadores de textos, ya que, como editar y trabajar sobre la información recolectada?!.

[4] De hecho los buscadores no son mas que grandes bases de datos sobre las cuales hay que recuperar la información. Esta claro que presenta una teoría estructural de fichado, organización y recuperación mas avanzada que la de un programa de recupero jurídico.

[5] Véase sobre este punto un articulo de Elisa M. Díaz de Vivar "Gestión informatizada de Expedientes. El camino que la justicia nacional en lo civil esta recorriendo". LL. Bs As. 14/12/99. Pág 1/3.
Algunos juzgados relativamente pequeños y con fondos suficientes han comenzado a colocar en Internet todos los despachos y proveídos del último día para que puedan ser consultados, tal es el caso de los tribunales provinciales de Pergamino (Bs As – Argentina) que junto al Foro local diariamente vuelcan en Internet la actividad diaria para poder ser consultada a través de la red. Véase www.pergamino.com./cap

3.3.- ¿Cómo enseñar?

Otra pregunta de respuesta difícil y compleja. La experiencia nos indica que solo las clases teórico-practicas dan resultados correctos. La practica sin teoría es sembrar sobre arena, el alumno no sabe que ni para que hace lo que esta haciendo.

La inversa lleva fatalmente al aburrimiento del educando y como docentes lo terminamos perdiendo.

El desarrollo de clases prácticas debe hacerse en laboratorios debidamente acondicionados y nuestra experiencia demuestra que se debe trabajar en grupos no mayores de 20 personas y solo una persona por maquina.

3.4.- ¿Cómo evaluar los resultados?

No existe en pedagogía campo de discusión tan amplio como el relativo a la evaluación[6].

Nosotros hemos optado por una evaluación de tipo teórica y una de tipo practica, ambas tienen la misma relevancia y se complementan.

Es imposible en este ámbito discutir todos los porque, cada docente, en cada casa de estudios tiene un sistema de acreditación de conocimientos y ello se debe a un criterio de oportunidad.

IV.- LA INFORMATICA COMO MATERIA OBLIGATORIA DE LA CARRERA DE ABOGACIA.

Uno de los compromisos fundamentales que debemos asumir desde nuestro rol de educadores es el de formar profesionales con capacidad para enfrentar al mundo globalizado de hoy con las herramientas adecuadas. Es por ello que, en la confección de los programas de estudios de la mayoría de las carreras que se cursan en la U.A.I., se optó por incluir como materia obligatoria a Informática Jurídica.[7] En el caso concreto de la carrera de Abogacía a través de los denominados "Talleres de Informática I y II".

La razón para tal inclusión, es la de dotar al alumno de los conocimientos básicos sobre el funcionamiento y utilización de la computadora como un instrumento al servicio de su actividad académica y en su futura labor profesional. Por otra parte, y para que ese aprovechamiento sea realmente pleno, tales talleres se encuentran comprendidos dentro de las materias que componen el primer año de la carrera buscando con ello su empleo y proyección durante todo el resto de la vida universitaria.

4.1.- La Informática entendida como una herramienta para el Abogado.

Un estudiante en una Facultad de Derecho estudia para ser abogado. Esta, que parece ser una verdad de perogrullo no es vista, a veces, con toda claridad por quienes tienen a su cargo la confección de los programas y/o el dictado de los cursos de Informática en las carreras de Abogacía.

No es extraño, entonces, observar que la estructura y contenidos que algunos docentes suelen otorgarle a la materia carezcan de la especificidad necesaria que requieren los usos del profesional del Derecho. Esto se traduce

---

[6] Existen diferentes formas, métodos y sistemas de evaluación. Normalmente cada casa de altos estudios sigue un sistema que se adapta a su situación histórica, pedagógica e institucional (cantidad de alumnos, antigüedad, ambientes, etc). En nuestras facultades se sigue una tradición de tipo oral y el examen en general es enciclopédico (el alumno debe demostrar al profesor conocimientos que se encuentran en los libros, obviamente memorizándolos, a veces sin entender un ápice de lo que esta manifestando). Esta modalidad no puede aplicarse para evaluar los procesos de aprendizaje en informática jurídica porque no obtendríamos resultados ciertos, en otras palabras el examen de enciclopedia en la materia *sería suicida*.

[7] A diferencia de otras casas de altos estudios en donde la enseñanza de la Informática Jurídica reviste el carácter de materia de cursado optativo para el alumno o bien sólo se reduce a un simple "curso de computación" paralelo semejante al que se dicta en institutos privados especializados.

en programas que no demuestran adaptación alguna a las necesidades del abogado pretendiendo convertirlo en un especialista en sistemas. En este sentido, por ejemplo, consideramos fútil someter al alumno a conceptos y fórmulas matemáticas o incursionar en sofisticados softwares de diseño propios de otras disciplinas más ligadas a las ciencias exactas pero que nunca tendrán para aquél una verdadera aplicación práctica.

4.2.- Articulación necesaria con otras materias.

Lo expresado en el punto anterior trae aparejado, inevitablemente, la necesidad de una adecuada interrelación entre la Informática y las demás materias integrantes del plan de estudios de la carrera de Abogacía, lo cual permitirá al docente informático[8], entre otras cosas, suplir su natural carencia de conocimientos legales a la vez que lo ayudará a comprender más cabalmente los requerimientos informáticos de la profesión.[9] En pocas palabras, se trata de incorporar a la Informática dentro del campo de operatividad del Derecho logrando, así, la tan ansiada integración cognoscitiva de ambas ciencias en una verdadera Informática Jurídica.

V.- LOS TALLERES DE INFORMATICA JURIDICA EN LA UAI.

5.1.- El Taller de Informática Jurídica I

5.1.1.-Enfoque conceptual y perfil a desarrollar.

Se pretende abordar a la Informática como herramienta para el desarrollo de las actividades del estudiante-hombre social y profesional del Derecho. Para ello, se considera de fundamental importancia lograr del alumno una comprensión y manejo de los recursos que ofrece la nueva tecnología, con miras a obtener de ella el máximo de su provecho para el ejercicio de las tareas propias del abogado.

5.1.2.- Correlatividades.

Como ya adelantáramos en párrafos anteriores, la ubicación del Taller de Informática Jurídica I dentro del conjunto de asignaturas que componen el primer año de la carrera, hacen que la misma carezca de una correlatividad anterior con otras materias, sí la tiene, en cambio, con su inmediata posterior, es decir, el Taller de Informática Jurídica II. Se encuentra, además, en estudio un proyecto para incorporar como materia optativa a Derecho Informático para cuyo cursado se exigiría la aprobación de los dos talleres mencionados .

5.1.3.-Objetivos de la materia.

La materia tiene, como objetivo primordial, capacitar al alumno en el conocimiento y dominio del ordenador, su funcionamiento básico, terminología técnica necesaria y empleo de los programas más difundidos para el desenvolvimiento de tareas específicas. Dentro de dicho esquema, el aprendizaje de los conceptos elementales de la ciencia Informática y de su especie, la Informática Jurídica, es fundamental a efectos de dotar a la práctica del sustento teórico necesario para su cabal comprensión.

---

[8] Nos referimos específicamente a los casos en que el dictado de la materia se encuentra a cargo exclusivo de docentes con conocimientos puramente informáticos.

[9] Taddei Elmi citado por el profesor Bauzá Reilly en su artículo reafirma estos conceptos al sostener que "... la Informática Jurídica... tiene carácter interdisciplinario y transversal. Se produce aquí un fenómeno parecido a lo que sucede con la "bioquímica", o la "ingeniería genética", donde se atraviesa en forma transversal una serie de disciplinas diferentes unas de otras, tomando de todas ellas principios, métodos, experiencias, y dando por resultado un campo nuevo de conocimiento y acción". Del mismo modo, Valle Fonrouge expresa que "... la tarea de la hasta ahora llamada Informática Jurídica fue y debe seguir siendo interdisciplinaria y es fundamental que tengamos plena conciencia de ello..." (VALLE FONROUGE, Marcelo F; Introducción a la Informática Jurídica, revista La Ley, tomo 1979-A, Sec. doctrina, pág. 793).

5.1.4.-Metodología de trabajo.

Teniendo en cuenta los objetivos generales propuestos, el trabajo se desarrolla por comisión y con clases serán teórico-practicas. Para ello, se emplean modernas técnicas pedagógicas como vídeo, transparencias y, obviamente, todo el equipamiento informático necesario con conexión a Internet en cada uno de las computadoras. Respecto de este último, la distribución se realiza de a un alumno por computadora con un máximo de 20 alumnos por curso.

5.1.5.-Criterios de evaluación.

La materia se aprueba con un examen final del tipo teórico-práctico. A dicha calificación final se suma el resultado de evaluaciones parciales y diversos trabajos prácticos realizados durante el transcurso del semestre además de la evaluación permanente del trabajo y la participación en clase con información periódica de la misma a los alumnos.

5.1.6.-Estructura de la materia.

La materia está estructurada en cinco unidades temáticas, cada una de las cuales se subdivide en diversos ítems para su tratamiento. Todas, en su conjunto, conforman una homogeneidad de conocimientos que permitirán una comprensión global y abarcadora de los diversos temas propuestos.

La primera unidad es introductoria a los conceptos de Informática, Computación, dato e información, la computadora, sus componentes (hardware y software) y evolución, Informática Jurídica, concepto, naturaleza, especies, etc.[10]

La segunda unidad adentra en los sistemas operativos y entornos operativos (comandos y funciones más comunes, compatibilidades, estructura de árbol, directorios, carpetas, archivos, etc.) con alusión a las diferentes clases de sistemas operativos existentes en el mercado.

La tercera unidad desarrolla el procesador de textos en su integridad, sus características, menúes, herramientas, etc. Por otra parte, y como complemento de la materia Derecho Procesal Civil, se trabaja sobre modelos de escritos judiciales sencillos buscando, así, comenzar a familiarizar al alumno, ya en el campo de la práctica, con la Informática Jurídica de Gestión.

La cuarta unidad desarrolla los conceptos básicos de planilla de calculo para su utilización en el campo de la abogacía.

La quinta y ultima unidad explora la utilización de programas complementarios para la administración y optimización del sistema (administradores y compresores de archivos, utilitarios en general, antivirus, etc.)

5.2.- *El Taller de Informática Jurídica II*

5.2.1.-Enfoque conceptual y perfil a desarrollar.

Habiendo el alumno recibido las bases generales de la Informática y la Computación, este Taller de Informática Jurídica II busca profundizar aquellos conocimientos para lograr un mejor perfil general del egresado.

[10] Consideramos que tales conceptos adquieren importancia al punto de ser la base a partir de la cual se desarrollan ambos talleres de Informática. No podemos enseñar Informática y menos aún Informática Jurídica sino sabemos antes de qué estamos hablando y cuál es su objeto de estudio como ciencia. Por otra parte, se intenta brindar al alumno un panorama que, mediante el repaso de los hechos más trascendentes, le permitan comprender la evolución de la Informática desde sus comienzos hasta nuestros días.

La materia se centra, esencialmente, en la Informática Jurídica Documental y de Gestión para lo cual se estudian y analizan los programas de manejo de bases de datos en general y de almacenamiento de información jurídica en particular. Asimismo, se dedica todo un capitulo al desarrollo de Internet y su aplicación en el campo de las ciencias sociales con especial referencia al ámbito jurídico.

5.2.2.-Correlatividades.

Como se señaló anteriormente, esta materia sólo posee una sola correlatividad anterior -el Taller de Informática Jurídica I- y carece de correlatividades posteriores.

5.2.3.-Objetivos de la Materia.

La materia tiene por objeto capacitar al alumno en el manejo de base de datos, diferentes clases, elementos que la componen, estructura, etc. Se pone especial énfasis en el manejo de programas de bases de datos que permitan la búsqueda y recuperación de información jurídica y la gestión integral de un estudio jurídico profesional.

Se pretende, como segundo objetivo, que el alumno aprenda a familiarizarse con la tecnología de redes, fundamentalmente de Internet, explorando sus recursos y aplicación directa al campo humanístico y jurídico.

5.2.4.-Metodología de trabajo.

Idem Taller de Informática Jurídica I.

5.2.5.-Criterios de Evaluación.

Idem Taller de Informática Jurídica I.

5.2.6.-Estructura de la Materia.

La materia se compone de cinco unidades temáticas relacionadas.

La primera unidad introduce al concepto de base de datos, diferentes clases, individualiza sus partes y sistemas de ordenación, etc.

La segunda unidad desarrolla los gestores de base de datos que dominan el mercado y muestra su funcionamiento estructural.

La tercera unidad se centra en el trabajo sobre bases y programas jurídicos. Esta unidad pone especial énfasis en el manejo de jurisprudencia informatizada, acelerando no solo el proceso de búsqueda sino también la calidad de la información que se encuentra.

La cuarta unidad acerca al alumno a la edición profesional a través de programas de presentaciones y diseño de publicaciones útiles en la tarea diaria de los abogados mediadores, en especial para la presentación de cuadros, esquemas y demás.

La quinta y última unidad se aplica al trabajo en redes con hincapié en Internet, sobre todo teniendo en cuenta que una buena parte de esta última no es sino una gigantesca base de datos materializada a través de millones de documentos almacenados en diferentes computadoras esparcidas por todo el mundo. Se destacan los principales recursos y servicios, los modos de uso y las diferentes formas de intercambio de información. Se reserva un acápite a la seguridad en la red.

VI.- CONSIDERACIONES FINALES.

A modo de una breve consideración final, sólo nos resta advertir que, lo que hemos intentado es tan sólo el esbozo de una visión sobre la enseñanza de la Informática en una Facultad de Derecho. Pueden existir infinitos puntos de vista, coincidentes o no con métodos o técnicas específicas que pueden variar según el caso o situación y, sin duda, es bueno que así sea pues toda nueva contribución ayuda al crecimiento. Lo que no debemos hacer es ignorar a la tecnología porque ella no ignora a nadie. Educar sobre el mundo técnico para aprender a servirse de él es otra manera de abrir las puertas que nos conducen a la libertad.

Fundamentos para la Autonomía del Derecho Informático en la República Argentina

Por Gustavo A. de Cara Corra (Argentina)

I).- INTRODUCCION

Desde hace algunos años atrás, los avances de la tecnología son cada vez más vertiginosos y modifican de un modo cada vez más acelerado la sociedad en que vivimos.

Hoy en los albores del año 2000, la informática y las telecomunicaciones, se presentan, asociadas con el concepto de las autopistas de la información, como determinantes en la construcción de una nueva sociedad, modificando hábitos y costumbres, y cambiando los tradicionales comportamientos y formas de trabajar, de disfrutar el ocio, e incluso de acceder a la formación y a la cultura.[1]

Desde el nacimiento la informática allá por los años cuarenta hasta el presente, se ha recorrido un largo camino en lo que a evolución técnica se refiere, ya que la sociedad moderna no sería posible, en muchos aspectos, sin la presencia del ordenador, es por ello que entre todos los adjetivos y denominaciones que se le han intentado atribuir al momento en que vivimos: era atómica, postmoderna, era espacial, etc., se ha llegado a la conclusión que estamos en presencia de la Era Informática o de la Información.

II).- LA ERA INFORMATICA O DE LA INFORMACION

Señala Alterini que la era de la sociedad industrial ha llegado a su fin, quizás el 6 de agosto de 1945 cuando el hombre demostró haber dominado la fisión nuclear, o quizás el 20 de julio de 1969, cuando arribó a la Luna.

Ha comenzado una nueva etapa en la Historia, se trata de una Era designada como Tecnológica, Tecnotrónica, Postindustrial, Neoindustrial, Superindustrial, de la Tercera Ola, Postmoderna, de la Información o de muchas otras manera posibles.[2]

De todas los adjetivos atribuidos para caracterizar el momento en que vivimos los que mejor se adaptan son el de *Era Informática o de la Información*, en especial este último, es bien conocido por todos el desarrollo levado a cabo en estos últimos años, en el ámbito de las Tecnologías de la Información, en especial la amplia difusión de Internet, ha influido de tal forma en nuestra sociedad que la gran mayoría de los campos del conocimiento se han modificado sustancialmente como consecuencia de esto, por ejemplo en el caso de la medicina (operaciones quirúrgicas a través de Web Cams en tiempo real, consulta de pacientes, etc), en la ingeniería e incluso en el derecho.

Hoy podemos afirmar que estamos inmersos en la sociedad de la información, pero antes de seguir detengámonos en el término información, *¿Qué se entiende por Información?*

Vittorio Frosini la define como: "*La capacidad de acumulación, elaboración y distribución de la experiencia humana por medio de un lenguaje que puede ser oral, mímico o simbólico, es decir que puede valerse de las facultades humanas del oído, de la vista o de la abstracción*".[3] Por su parte Pierre Catalá entiende por información: "*Todo mensaje comunicable a otro por cualquier medio*". Haciendo referencia también a la existencia de un derecho a la información que puede entrar en conflicto con el derecho a la información propio de un Estado de derecho en el cual se reconoce el pluralismo de la información y la libre investigación científica.[4]

---

[1] CARRASCOSA LOPEZ, Valentín, Tecnologías de la Información: Reflexiones sobre su Regulación Jurídica, en VI Congreso Iberoamericano de Informática y Derecho, Libro de Ponencias, (Montevideo 1998), Pág. 364.

[2] ALTERINI, Atilio Aníbal, Desmasificación de las relaciones obligacionales en la Era Postindustrial en L.L. 1989 - C - 955.

[3] FROSSINI , Vittorio, Informática y Derecho, trad. Por Guerrero y Ayerra Redin, Ed. Temis S.A., (Bogotá, Colombia 1988), Pág. 27.

[4] CATALA, Pierre, Ebauche d'une theorie juridique de l'information, Recueil Dalloz Sirey, 16º cahier, Chronique, 1984, citado en: CORREA, NAZAR ESPECHE, CZAR DE ZALDUENDO, BATTO, Derecho Informático, Ed. Depalma, (Buenos Aires, 1994), Pág. 288.-

Siguiendo el pensamiento de Frosini, este autor expone como la civilización del hombre comienza con el intercambio de informaciones entre ellos y como va evolucionando con el correr del tiempo, en un primer momento, el mensaje se brindaba en forma directa, inmediata e individual, luego se extiende al grupo y posteriormente a un grupo cada vez más amplio. La invención del lenguaje figurativo, representa un paso importante pues a través del signo, luego la escritura, el mensaje se plasma en la roca y se separa del hombre para transformarse en cosa, lo que permite comunicar a los presentes con los ausentes y a los vivientes con los muertos que les había precedido y con los vivientes que le seguirán. El paso más importante lo marca la aparición de la escritura impresa con caracteres móviles sobre papel, permitiendo la aparición de la prensa diaria.[5]

Podemos afirmar, que la información no es algo nuevo, sino que existe desde los orígenes de la humanidad, y le ha servido al hombre entre otros propósitos, para alertar a sus semejantes de los peligros que los acechaban, indicarles donde buscar alimento, difundir a otros sus ideales o las noticias de la ciudad, etc.

Lo que ocurre es que hoy la información se presenta con caracteres propios que realzan su importancia en el esquema de la sociedad. Su cantidad, variedad y rapidez de circulación, necesidad de la misma en cuanto a la toma de decisiones, por último la posibilidad de su tratamiento automático, constituyen las piedras fundamentales en las cuales se asienta este extraordinario fenómeno. Se ha dicho que la economía del siglo XIX estuvo dominada por el desarrollo de las fuentes de energía, la del siglo XX, y más particularmente su segunda mitad, se caracterizará, en la historia económica como el siglo de la información.[6]

La comunicación humana, ha cambiado, después de pasar de la oralidad, a la escritura manual y luego de esta a la escritura impresa, en la actualidad es la comunicación teletransmitida (Televisión, Radio, Ordenador), la que ha superado todo los límites de tiempo, espacio y lugar.

No cabe duda que este nuevo fenómeno de la Era de la Informática o de la Información, es necesario regularlo jurídicamente, para que la ofensiva tecnológica no aplaste al hombre aun cuando, por razones de progreso, se vea obligado a cambiar de hábitos y de sus conceptos tradicionales.

Dice el jurista español Valentín Carrascosa López: junto con las incuestionables ventajas derivadas de las inmensas posibilidades de conocimiento, actuación y comunicación que permiten la navegación por el ciberespacio, que no es otra cosa que un microcosmo digital en el que no existen fronteras, distancias ni autoridad centralizada, la Informática, Internet, etc. han hecho surgir graves motivos de inquietud (pornografía, propaganda de bandas terrorista, etc.), que han llevado a millones de ciudadanos a poner de manifiesto los peligros que entrañan determinadas manipulaciones de las nuevas tecnologías de la información.[7]

III).- DEFINICION DE INFORMATICA

Antes de entrar de lleno en la noción de derecho informático y la informática jurídica, se hace necesario arribar a una definición de Informática.

Altmark sostienen que la informática puede definirse como: *"La disciplina que estudia el fenómeno de la información, y la elaboración, transmisión y utilización de la información aunque no necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos .[8]"*

Por su parte Federico Fumis, ensaya la siguiente definición: *"Es la aplicación racional y sistemática de la información para el desarrollo económico, social y político."*[9]

---

5 FROSINI, Vittorio, op. Cit., Pág. 29 y ss.

6 TUBOL, Frèdèrique, El Software: Análisis Jurídico, trad. de Luis Moisset de Espanés, Ed. Zavalía, (Buenos Aires, 1990), Pág. 11.

7 CARRASCOSA LOPEZ, Valentín, op. cit., Pág. 365.

8 ALTMARK, Daniel Ricardo, La Etapa Precontractual en los Contratos Informáticos, en Informática y Derecho, Vol. I, Ed. Depalma, (Buenos Aires, 1987), Pág. 6.

9 FUMIS, Federico, Informática y Derecho de Daños, en Revista Electrónica de Derecho Informático (REDI), Derecho.org, 1999.

El Centre de Recherches Informatiques et Droit de Facultès Universitaires de Namur sostiene: *"Son los aspectos de la ciencia y la tecnología específicamente aplicables al tratamiento de la información y en particular, al tratamiento automático de datos."*[10]

En un sentido similar Guastavino entiende por Informática: *"El tratamiento automático de la información a través de elaboradores electrónicos basados en las reglas de la cibernética."*[11]Y define a esta última, como la rama de la ciencia que estudia los sistemas de control y especialmente de autocontrol en organismos y máquinas.

La informática es una herramienta, que sirve para facilitar al hombre sus tareas cotidianas, permitiéndole crear, comunicarse, educarse, realizar transacciones comerciales, relacionarse con otros hombres, etc..; es por ello que decimos que la Informática es *"La herramienta que sirve para el almacenamiento, recuperación, distribución, organización, expresión y comunicación de la Información, por intermedio de un sistema automático de tratamiento de datos."*

IV).- INFORMATICA JURIDICA Y DERECHO INFORMATICO: CONCEPTOS

La Informática ha penetrado en el mundo jurídico de dos formas bien diferenciadas, por un lado como herramienta para el jurista en el tratamiento de la información jurídica (Informática Jurídica) y por otro la Informática plantea nuevos problemas que derivan de su utilización y desarrollo los cuales necesitan ser resueltos por el derecho (Derecho Informático).

La Informática Jurídica puede ser definida como: *"aquella rama de la Informática que es puesta al servicio del abogado, jurista o juez y que tiene como finalidad brindar un mejor tratamiento de los datos jurídicos, optimizando la labor diaria de los actores jurídicos."*

Por otro lado tenemos que el Derecho Informático es: *"el conjunto de normas, principios e instituciones jurídicas que regulan las relaciones que surgen de la actividad informática, evitando que la tecnología pueda contraponerse a los derechos fundamentales del hombre, regulando lo relativo a la instrumentación de las nuevas tecnologías de la información, el uso y comercialización de los bienes informáticos, y la transmisión de los datos".*

V).- EL DERECHO Y LA SOCIEDAD DE LA INFORMACION

¿Cual es el papel del Derecho en esta nueva Sociedad de la información?

El Hombre de Derecho ante esta nueva realidad social, puede tomar dos caminos: A).- Aceptar y someterse al derecho tal como está regulado, sin tener en cuenta la discrepancia entre la evolución tecnológica y la reglamentación jurídica. B).- Desarrollar una nueva legislación adecuada a los cambios que sufre la sociedad, formulando propuestas a fin de que el Derecho asuma nuevas formas que no sólo obstaculicen el uso de las nuevas tecnologías, sino que lo regulen adecuadamente, revisando y adecuando las viejas leyes a las necesidades y situaciones jurídicas que van apareciendo con las nuevas tecnologías.[12]Creemos que esta última es la actitud que debe tomar el jurista de hoy, ardua tarea, pero no imposible.

El intercambio intenso de mercaderías más allá de los aranceles y las costumbres, la simbiosis de las culturas o mejor dicho su adaptación y asimilación en nuevos contextos, la velocidad con que se transmiten informaciones de toda índole, forman parte de esa idea general que conocemos como globalización y que pone de manifiesto que la solución jurídica, de estos problemas sea todavía confusa y enrarecida, ya que la rapidez con que se suce-

---

[10] ALTMARK, Daniel Ricardo, op. cit., Pág. 6.
[11] GUASTAVINO, Elías P., Responsabilidad Civil y otros problemas jurídicos en computación, Ed. La Rocca, (Buenos Aires, 1987), Pág. 25.
[12] CARRASCOSA LOPEZ, Valentín, op. cit. Pág. 365

den los cambios obliga a las personas y a las organizaciones a realizar modificaciones constantes a fin de no perder el contacto ni quedar al margen de este flujo de innovaciones tecnológicas, de aquí que las diferentes ramas del derecho se vean afectadas.[13]

Dice José Luis Montoto Guerreiro, todas las actividades humanas como: el comercio, la investigación, el juego, el trabajo, el estudio de las organizaciones, las guerras, etc; han incorporado a sus vidas el nuevo elemento cultural (entiéndase la Informática - nota del Autor) desde hace aproximadamente cuarenta años.

Continúa diciendo este autor que en este contexto, emerge la economía digital, como base de comercialización de productos en un mundo globalizado; o Internet, que podríamos llamar, sin temor a equivocarnos, la innovación básica, más trascendente desde la imprenta, que transformará toda la actividad humana en los años venideros ya que dependerá de la implementación correcta del enfoque Internet/Extranet en las organizaciones gubernamentales o privadas, el éxito, estancamiento o desaparición.[14]

Podemos afirmar que cada una de las disciplinas jurídicas, se encuentran tocadas, en más o en menos con el objeto cultural computador u ordenador, podemos citar como ejemplos:

1).- En el Derecho Comercial surge la contratación electrónica y los elementos, requisitos y efectos, etc., de los contratos telemáticos.

2).- En el Derecho Constitucional, la protección de la vida privada, donde existiendo datos aislados sin autorización de sus titulares (que ya existen en distintas bases de datos, privadas y públicas que si no determinan nada, dibujaríamos un perfil psicológico de preferencias, tendencias, intereses, de uno o varios segmentos de la sociedad minimizando al máximo la libertad de elección, con todas sus implicancias jurídicas.

3).- En el Derecho Civil: la determinación de la responsabilidad del titular del fichero electrónico respecto del uso no autorizado o inexacto que fuere generador de daño físico, patrimonial o moral.

4).- En el Derecho Laboral, con la aparición de las Bolsas de Trabajo en Internet, donde se ofrecen en conjunto aproximadamente 500.000 puestos de trabajo. Bases de Datos conteniendo el currículum vitae del oferente. El teletrabajo donde hoy existen en este régimen 2.400.000 trabajadores en Europa.

5).- Etc.[15]

De lo apuntado, podemos deducir que el ordenador plantea nuevos problemas de tipo jurídico con los que se han de enfrentar los hombres dedicados a la creación, interpretación y aplicación de las leyes, es lo que se conoce como Derecho Informático, que a raíz de todos estos nuevos fenómenos sociales y jurídicos, va adquiriendo carta de naturaleza, a pesar de encontrarse por ahora en un estado embrionario, lo cual no implica que no existan numerosas disposiciones legales, jurisprudencia y muchos textos doctrinales que se han hecho eco de estas nuevas cuestiones jurídico - sociales.

VI).- NECESIDAD DE AUTONOMIA DEL DERECHO INFORMATICO

Vamos a tratar en este punto una cuestión arduamente debatida entre los doctrinarios de esta nueva realidad jurídica (el Derecho Informático) , la Necesidad de Autonomía del Derecho Informático, para ello deberemos preguntarnos, ¿cuáles son las características que debe reunir una rama del derecho para adquirir autonomía?.

---

13 Ibídem.

14 MONTOTO GUERREIRO, José Luis, Los Sistemas y Tecnologías de la Información a fines del Siglo XX y sus puntos de Contacto con el Orden Social Justo, en Revista Electrónica de Derecho Informático (REDI), Derecho.org, 1999.

15 Ibídem

Antes que nada debemos detenernos y hacer una salvedad, el Derecho es uno, y sólo se lo divide en ramas para facilitar una mayor y mejor adecuación de sus normas a determinadas formas de conducta, en función de fines concretos.

Dice al respecto Dromi: "Creer que cada rama del derecho es independiente, es suponer que hay varios derechos, y el derecho es uno. Las relaciones entre las distintas disciplinas jurídicas, describen los principios unificadores, capaces de determinar una unidad sistemática y una coherente analogía jurídica entre las varias ramas de un único ordenamiento positivo, que ofrece algunos institutos comunes y fronterizos a más de uno de sus ordenamientos especiales."[16]

Podemos afirmar que lo que caracteriza y da autonomía a una rama del derecho, es que esta se oriente en cuatro aspectos:

A).- Autonomía Legislativa: es decir que tenga una legislación especificada, normas propias, a las cuales se pueda recurrir en caso de necesidad, no necesariamente debe estar codificada, como sería el Código Civil o Penal, sino que bien puede tratarse de una Ley o un conjunto de Leyes. Esta leyes deben abarcar la mayor cantidad de situaciones posibles que en la materia se presenten, esto se hace necesario para tener que evitar recurrir en forma permanente a las normas de carácter general.

B).- Autonomía Académica: es el estudio particularizado y pormenorizado de la materia, enseñado en forma separada, con una cátedra propia, que exponga sus principios en forma clara y ordenada y desde la cual se puedan hacer investigaciones sobre su objeto y conceptos.

C).- Autonomía Jurisprudencial: se refiere a la existencia de instituciones propias que no se encuentren en otras áreas del derecho, como la existencia de Tribunales específicos y magistrados especializados en esa rama jurídica.

D).- Autonomía Científica: esto significa que existan investigaciones, doctrinas, que esté organizada como un sistema relativamente completo de normas y principios, a los cuales se pueda recurrir en forma excluyente en caso de dar solución a un problema de la materia tratada en esa rama, es decir que lo que se trata es que la rama pueda valerse por sí misma, independientemente del auxilio del resto del ordenamiento jurídico positivo.

La doctrina mayoritaria en nuestro país sostiene la negación de la autonomía del Derecho informático, esta se basa en los siguientes fundamentos:

1).- Inexistencia de un conjunto de normas jurídicas, en forma de código o de ley, o leyes ordenadas relativas al derecho informático.

2).- No todas las Universidades Argentinas tienen cátedra de derecho informático.

3).- Tampoco existen tribunales propios de conocimiento.

4).- Al no darse los supuestos anteriores, tampoco existe una estructura más o menos orgánica de principios de manera tal que pueda recurrirse a ellos a los fines de hacer cerrar los contenidos de la rama.

Para esta parte de la doctrina la no existencia de estos principios trae la lógica consecuencia de la falta de los tres elementos restantes necesarios para componer la autonomía de una rama, por lo tanto descartan de plano toda posibilidad de considerar al Derecho Informático como una rama autónoma, recayendo en que el mismo se descompone en un conjunto de normas totalmente aisladas provenientes de distintos ámbitos (penal, civil, comercial), y en muchos casos no existe previsión jurídica para los problemas que plantean las nuevas tecnologías. [17]

---

[16] DROMI, Roberto, Derecho Administrativo, 3° Edición Actualizada, Ed. Ediciones Ciudad Argentina, (Buenos Aires, 1994), Pág. 90.

[17] ZABALE, Ezequiel y BELTRAMONE, Guillermo, Acerca de la Autonomía del Derecho Informático, en Revista Electrónica de Derecho Informático (REDI), derecho.org, 1999.

Pese al panorama desalentador que expresa esta doctrina, podemos sugerir una postura más flexible, y adecuada a las necesidades que la realidad jurídico - social hoy nos reclama, la cual no podemos dejar desprotegida, por el mero hecho de no darse unos parámetros rígidos y anticuados, que sólo sirven de excusa, para relegar al Derecho Informático a la sombra de otras disciplinas jurídicas, siendo que ya estamos frente a situaciones fácticas que hacen imperiosa la necesidad de regular jurídicamente de una vez por todas, esta nueva y creciente realidad jurídica, que es el Derecho Informático.

Generalmente el nacimiento de una rama jurídica surge como consecuencia de los cambios sociales, reflejados en las soluciones normativas por el transcurso de los años. Pero resulta que en el caso de la informática no hubo ese transcurrir del tiempo en los cambios sociales, sino que el cambio fue brusco y en poco tiempo, se lograron de esta manera sociedades altamente informatizadas que sin la ayuda actual de la informática colapsarían.

No obstante, a pesar de que esta situación existen países desarrollados como España, en los que si se puede hablar de una verdadera autonomía del derecho informático, haciendo la salvedad de que esta ciencia como rama jurídica apenas nace y se está desarrollando, pero se está desarrollando como una rama jurídica autónoma.

Por lo tanto no hay excusa, ni siquiera para un país donde el grado de informatización sea bajo para que se obvie la posibilidad de hablar del derecho informático como rama jurídica autónoma del derecho, si bien se puede llegar a ella por la integración de las normas jurídicas, sino también por la heteroaplicación, cuando en un sistema jurídico existan vacíos legales al respecto.18

Pensemos que no sólo esta rama del derecho necesita de la integración con otras, sino que todas las ramas del Derecho están intervinculadas entre ellas , tomemos como ejemplo el Art. 16 del Código Civil Argentino, que reza:" Si una cuestión civil no puede resolverse, ni por las palabras, ni por el espíritu de la ley, se atenderá a los principios de las leyes análogas; y si aún la cuestión fuere dudosa se resolverá por los principios generales del derecho, teniendo en consideración las circunstancias del caso", como vemos el Derecho Civil, tal vez la más amplia de las ramas del derecho, también necesita a veces recurrir a la analogía y los principios generales del derecho, sin que ello quite en lo más mínimo el carácter de rama autónoma del derecho.

VII).-CONCLUSIONES

Es por ello que sostenemos que si es posible la Autonomía del Derecho Informático, siempre teniendo muy presente que estamos ante una ciencia embrionaria, poco conocida y entendida por los juristas, que necesita nutrirse de otras ramas, pero que tiene un objeto propio de estudio, complejo y diferente, que son todas las cuestiones que plantea el uso del ordenador y las nuevas tecnologías, que si bien no existe legislación específica, ello no implica que el legislador esté ausente de esta realidad, y que en poco tiempo más se elaboren normas jurídicas que traten en forma exclusiva, la problemática que plantea el Derecho Informático, tampoco están indiferentes los claustros universitarios quienes ya están incorporando en sus planes de estudio la asignatura Derecho Informático, Informática Jurídica o Derecho de las Altas Tecnologías de la Información, los juristas tampoco se han quedado atrás, con su aporte a numerosas publicaciones y congresos de Informática y Derecho, etc.

18 PEÑARANDA QUINTERO, Héctor Ramón, La Relación Derecho - Informática como Asignatura para Juristas e Informáticos, en VI Congreso Iberoamericano de Derecho e Informática, Libro de Ponencias, (Montevido, 1988).

Enseñanza del Derecho Informático y del Derecho Informatizado en un Programa de Enseñanzas no Regladas de la UNED

Francisco Eugenio Díaz / Araceli Oliver (España)
Universidad Nacional de Educación a Distancia (UNED). Madrid. España

Unas primeras palabras de agradecimiento a los organizadores y a los asistentes. Después, otras de excusa por si lo que pase a decir es otra cosa de lo que ustedes esperan y merecen, o incluso es cosa que de alguna manera ya saben.[1]

Habré de atenerme a contar la limitada realidad que conozco: ésta se refiere a la UNED [esto es, la Universidad Nacional de Educación a Distancia, de España, con su llamada Sede Central en Madrid] y, más concretamente, a unos cursos de lo que se denomina Enseñanza Abierta referidos: uno, a INFORMÁTICA JURÍDICA y otro, a INFORMÁTICA Y DERECHO: DERECHO INFORMATICO.

INTRODUCCION:

Información y tratamiento industrial de la información. Sociedad de la información digitalizada.

Partimos de un concepto base, la información, principio y fundamento del Derecho informatizado y del Derecho informático. No deja de ser curioso que al que modela la arcilla se le dice en latín "figulus" y a lo propio o realizado por el alfarero se lo llame figulinus, o, en femenino, figulina. Modelar, configurar, informar, formar, tienen todas la misma connotación, la misma referencia a *forma* y a figura.

La información es, como se sabe, un conjunto de signos significativos que se pueden fijar en algún soporte material y que se pueden difundir o transmitir a alguna parte mediante los oportunos canales de difusión o de transmisión. Lo que signifiquen los signos de información dependerá naturalmente del correspondiente *código*, de la correspondiente *tabla* de equivalencias en la que se establecen de antemano las oportunas correlaciones entre signos significantes y mensajes significados (ideas, sentires, mandatos, por ejemplo).

Los humanos nos entendemos con el lenguaje humano, de los sonidos humanos que desde muy antiguo, desde la invención del lenguaje escrito, se han venido representando por medio de los caracteres de escritura: las letras del alfabeto esencialmente.

Pero desde que aparecieron las máquinas de tratar información, las máquinas (tanto para "reconocer" las instrucciones que les damos los humanos como para utilizar, también ellas, nuestras letras del alfabeto en su "versión máquina"), desde que aparecieron las máquinas de tratar información, decimos, está en circulación lo que se llama el lenguaje máquina, en virtud del cual, por ejemplo, la letra A se representa con la siguiente ristra de caracteres binarios, ceros y unos: 010001.

A partir de la transformación de los signos del lenguaje humano en signos de lenguaje máquina la información, constituída por señales de información, admite ya un tratamiento industrial o industrializado: puede ser procesada por las máquinas, lo que significa que puede ser almacenada y reproducida "en cantidades industriales", con poco costo y con poco o ningún esfuerzo humano, y que puede ser igualmente "elaborada" (esto es reconformada, o formalmente retocada, o remodelada, o interrelacionada con otra, o de cualquier manera "tratada por la máquina de tratar información").

---

[1] Parodiando al autor de El Quijote (que a pesar de haber querido producir con su escrito el mejor de sus libros, le salió, expresa, un hijo avellanado y disminuido) bien hubiéramos querido poder servir a ustedes la mejor de las experiencias en cuanto se refiere a la enseñanza de "La Informática y el Derecho". El que no sea éste el caso no impide que aceptemos con gusto la ocasión de suscitar un posible coloquio sobre el tema.

Los progresos de la técnica han traído el ordenador, la fibra óptica, la red de nodos de información, el libro digital autorrecargable, la firma electrónica y las transacciones comerciales on line. Todo ello comporta un "tratamiento automatizado de las señales de información", que creemos es expresión más precisa que la usual de "tratamiento automatizado de la información", que no es sino un sobreentendido de la primera.

Cuando se habla de las nuevas tecnologías, sin más, también se está sobreentendiendo que se habla de las "nuevas tecnologías del tratamiento automatizado de las señales de la información". Eso por no añadir que son en realidad de nuevas técnicas de lo que se habla y no de la ciencia sobre nuevas técnicas.

De todos modos, la información digitalizada (convertida en cadena de dígitos binarios, en ristras de ceros y de unos) es un hecho; como lo es la producción y reproducción industrial, con procedimientos industriales (esto es, rápidos, baratos, económicos, masivos).

Las consecuencias económicas, sociales y culturales de este hecho todavía no las podemos prever con claridad. Lo cierto es que *unos nuevos hábitos, unas nuevas necesidades*, unas nuevas posibilidades están ya ahí: son los hábitos, las necesidades y las posibilidades de la que es reconocida como sociedad digitalizada.

¿Qué significa para un jurista, para un estudiante de derecho, para un profesor de derecho, para un juez y, en general, para un operador del derecho, esta nueva sociedad invadida y moldeada por el tratamiento industrial de la información?. Por lo pronto el universitario debe ser, con frase del eminente médico humanista español Laín Entralgo, "un hombre de su tiempo". Y, habría que añadir, el profesional de hoy no debe desconocer las actuales técnicas de su profesión. Hoy la profesión de operadores del Derecho requiere un cierto conocimiento de la recíproca implicación entre "Informática y Derecho"

1.- EL DERECHO COMO LENGUAJE.

Informatización del Derecho. Escritura y videoescritura.

Los caracteres alfabéticos (alfanuméricos, con mayor precisión) son la forma bajo la que el Derecho, a través de normas que se escriben, se manifiesta y se fija. Como es sabido, el Derecho, aparte de ser un *valor* que se vive y aparte de ser un *hecho* que se observa, es también unos signos o señales que se escriben, es decir, un conjunto de señales de escritura, un *lenguaje*. El Derecho es "información escrita", esto en la sociedad del Derecho de los códigos y aún antes: en la sociedad de los usos o costumbres jurídicas, del derecho consuetudinario *sí*, "creado" por la costumbre, pero "vertido" también a papel mediante la escritura de tales usos y costumbres [el ejemplo de la Ley de las Doce Tablas, a mitad de camino entre el Derecho consuetudinario y el Derecho escrito, avala lo que acabamos de decir].

Definitivamente, no se concibe la profesión de jurista (profesor, juez, abogado, etc.) sin la herramienta del lenguaje. El Derecho se expresa con el lenguaje, se defiende con el lenguaje, se hace operativo por medio del lenguaje.

Desde que en los trámites procesales del Derecho romano apareció la fórmula, el escrito en el que queda planteado el litigio (por obra de la Lex Aebutia de formulis de cerca del 130 a. C.) el texto escrito cobra un valor fundamental en el proceso. Pero también desde las más antiguas codificaciones (la del Edicto pretorio, del 130 d. C., y la del Digesto de Justiniano en el siglo VI de nuestra era) hay un reconocimiento explícito del valor de la literalidad de la norma jurídica, del valor del Derecho escrito y, por así decirlo, puesto en limpio.

La tradición oral de los procesos es un hecho; pero la fijación por escrito de las actuaciones procesales no le va a la zaga. Y en nuestra cultura de la palabra impresa, tras la invención de la imprenta naturalmente, la labor de los operadores del Derecho, como ahora es moda decir, es impensable sin la escritura: afortunadamente ya no de rasgar el papel con la pluma de un ave sino de administrar las marcas digitales sobre el folio electrónico que aparece en pantalla.

Se trata de que el jurista de hoy, como el de ayer era hasta hace poco un escribano manual y después, hasta cierto punto, un mecanógrafo, aprenda a ser un usuario de los programas procesadores de texto, o, dicho de otro

modo, un conocedor práctico de la videoescritura que es lo que se dice en Italia de la escritura por medio del ordenador, del "elaboratore" [de información, se entiende].

2.- TRATAMIENTO DE TEXTOS EN EL AMBITO DEL DERECHO

La funcionalidad del texto jurídico bien expuesto.

La estética no es un antivalor en el ámbito de los "papeles" de Derecho, por más que se censure en ocasiones la belleza literaria de los escritos jurídicos; esa belleza "retórica" no tiene nada que ver, a nuestro entender, con la estética funcional de un documento: sus apartados, sus frases cortas, sus epígrafes, su terminología depurada y rigurosa, nada ambigua, su prudente administración de subrayados, mayúsculas y cursivas. Todo eso está al alcance de quien use con conocimiento y con tino el ordenador y se esfuerce en concebir un escrito preciso, claro y presentado con gusto, con esmero, con la cortesía de los aspectos formales que su destinatario, el lector, merece y hasta necesita para entenderlo pronto y bien.

Aparte de este servicio de utilidad que el escrito bien formado ofrece al lector a quien va dirigido, hay otra razón en favor de la enseñanza y aprendizaje práctico de la escritura con ordenador: la propia formación del jurista. La enseñanza no comprende sólo el hecho de impartir conocimientos sino también la tarea de facilitar la adquisición de *destrezas*. De ahí que un programa de enseñanza sobre Informática Jurídica deba comprender el aprendizaje de cómo escribir con el ordenador, como adiestrarse en la escritura electrónica.

El material suministrado a los alumnos de este programa incluye desde luego lecciones sobre Windows, como plataforma de programas o programa del sistema operativo, y sobre Word, un estándar de procesadores de texto.

Los criterios seguidos para la confección de este material han sido, por una parte la secuencialidad de exposición de contenidos (lo que conlleva un índice de cuestiones a tratar y de pasos sucesivos a seguir) y, por otra, la sencillez y claridad del lenguaje. Unas listas de libros de posible (pero no imprescindible) consulta completan las explicaciones. Las prácticas que cada alumno realice después determinarán su grado de aprovechamiento en este punto, lo que se manifiesta naturalmente en la exposición de los trabajos que es necesario presentar.

Sobre todas las ventajas que se quieran ver en la utilización de los programas de procesamiento de textos hay un no pequeño inconveniente: las vueltas de tuerca de un perfeccionamiento sucesivo que admite siempre un nuevo detalle de perfección.

La indiscutible ventaja de lo escrito con ordenador es su capacidad de reutilizaciones y actualizaciones y su garantía, si somos precavidos, de recuperarlo a voluntad, con tal que hayamos sabido nombrarlo de manera razonable (o, basta ahora ya, que recordemos alguna de sus palabras que consten en el texto y no sean precisamente del montón sino particulares).

Con todo, somos partidarios de organizar la información en una decena de carpetas (de la carpeta 0, obras generales a la carpeta 9, ocio y negocio, pasando por las restantes entre las que se encuentra la carpeta 6 de Sociedad y Derecho. De esa carpeta 6 han de colgar las subcarpetas y documentos de contenidos jurídicos)[2].

No cabe duda de que el gusto por el orden, por la jerarquización de los niveles de registro y recuperación de información, por el nombramiento pertinente de los documentos, sobre ayudar a configurar la mentalidad lógica del jurista, estimularán su sentido de la armonía y harán de él un ser preciso, amante de lo verdadero y de lo justo, de lo razonable, un verdadero "prudente del Derecho".

---

[2] El primer nivel de clasificación de los conocimientos lo determinamos del siguiente modo: 0, Diccionarios y colecciones; 1, Ideas y creencias; 2, Lengua y Literatura; 3, Música y Artes; 4, Historia y Geografía; 5, Educación y Universidad; 6, Sociedad y Derecho; 7, Naturaleza y Vida; 8, Ciencia y Técnicas; 9, Ocio y negocio.

Todavía ofrece una ventaja más la videoescritura aplicada a los escritos jurídicos: la posibilidad de cooperación, de intercambio de información entre profesionales del Derecho, gracias a la homologación formal de los productos conseguidos con esta maravillosa herramienta de escritura que es la escritura con el ordenador.

3.- EL DERECHO Y LAS BASES DE DATOS.

Informática jurídica documental

La escritura de la norma jurídica supuso una cierta garantía para los sujetos a los que iba destinada, la garantía de su publicación, de su conocimiento publicitado. Mas la consulta de un amplio repertorio de derecho escrito soportado en papel aun puede ser penosa, lenta, insegura antes de que se invente la informática documental, esto es, la búsqueda de cadena de caracteres y, de resultas, de documentos, guardados en archivos de información tratada industrialmente, automatizada en cuanto a su registro y en cuanto a su recuperación.

Con los programas de gestión de bases de datos documentales de que actualmente disponemos, la recuperación de documentos jurídicos (artículos de un código, legislación puntual sobre cualquier cuestión, sentencias jurisprudenciales o aun repertorios bibliográficos) puede hacerse al instante y con toda garantía.

Como hemos dicho en alguna otra ocasión[3], "las condiciones para que un depósito de información constituya una base de datos son las siguientes:

1º, que se trate de información electrónica, digitalizada, procesada por una computadora;

2º, que se trate de información estructurada de algún modo, registrada conforme a ciertos criterios;

3º, que se trate de información gestionada por un programa de ordenador.

En España existen diferentes bases de datos jurídicas tanto públicas[4] como privadas[5], ya sean de legislación, ya de jurisprudencia, ya incluso de repertorios bibliográficos.

Lo que falta, y especialmente en el colectivo de juristas que ha sobrepasado cierta edad, es una cierta cultura informática que permita el empleo de las herramientas de búsqueda de información propias de la era digital en la que ya estamos inmersos.

Con nuestros programas de "Informática y Derecho: Informática Jurídica y Derecho Informático" se trata de eso: de capacitar para el empleo de las herramientas de bases de datos jurídicas y aun para el conocimiento y manejo de programas de gestión de bases de datos [6].

Respecto a la debatida cuestión de si es preferible organizar la información de modo que se permita la búsqueda por Tesauros o dejarla sin estructurar para que baste la búsqueda llamada por texto libre, nos permitiremos abogar por la *estructura de la información jurídica*.

La propensión a sistematizar algo (en nuestro caso, a clasificar los tramos de información conforme a un sistema, conforme a la estructura de árbol, esto es, en ramas y subramas) sabemos que conlleva el riesgo de lo rígido, de lo artificial, de la pura divagación. No somos partidarios, sin embargo de la información caótica: toda información, todo documento, toda unidad de información necesita un cierto orden interno; y también un orden dentro del todo en que se integra. Por eso creemos en los *esquemas* de un libro, en los *sumarios*, en los *epígrafes* de un ar-

---

[3] Informática Jurídica, Uned 1994, págs. 147 y ss.

[4] Las del *Boletín Oficial del Estado (BOE) principalmente.*

[5] Aranzadi, Actualidad/La Ley, El Derecho, Lex Nova, etc.

[6] Como el Access de Microsoft, por ejemplo.

tículo, en la lógica estructura de los *programas* de asignaturas (el mejor de los cuales serìa aquél que pudiera ser memorizado sin dificultad por los alumnos que lo utilicen: tal sería su sencillez, su lógica interna de apartados, temas y epígrafes; decimalizados y en paralelo, por lo demás).

Creemos que las "recuperaciones de documentos" jurídicos de una base de datos se deben poder hacer de estos dos modos: tanto desde el modo de búsqueda por epígrafes y palabras de un *Tesauro,* como por el modo de búsqueda del llamado *texto libre* o sin estructurar.

4.- "INFORMATICA JURIDICA".

Una experiencia docente

El curso denominado "Informática Jurídica" en la UNED pertenece al grupo de las llamadas Enseñanzas no regladas que se imparten en esta Universidad.

La Enseñanzas regladas se corresponden con los estudios de alguna de las Licenciaturas, Ingenierías o Ingenierías Técnicas que, ajustándose a determinados currículos o programas desembocan en la obtención del correspondiente Grado de Licenciado, Ingeniero o Ingeniero Técnico según el caso. En la UNED estos Enseñanzas regladas dependen del Vicerrectorado de Ordenación Académica y Profesorado, que es a quien corresponde el control y seguimiento de los respectivos planes de estudios.

Las llamadas Enseñanzas no regladas comprenden un tipo de cursos autónomos, sueltos, con valor en sí mismos, que se ofertan a las personas interesadas en sus respectivos contenidos y para cuya matriculación y pruebas de evaluación puede no necesitarse una titulación previa. De este tipo de enseñanzas no regladas se ocupa el Vicerrectorado de Educación Permanente que en nuestra Universidad tiene gran importancia y variadas atribuciones, entre las que se incluyen la competencia en materia de Cursos de Formación del Profesorado en ejercicio y en materia de Cursos de Enseñanza abierta; para la inscripción en estos últimos no se exige titulación previa.

Lo que se obtiene al final de cualquiera de los Cursos de Enseñanzas no regladas es un Diploma oficial de la Universidad que es muy estimado para el currículo del alumno y que, en ocasiones, es tenido en cuenta para determinar la puntuación otorgada a los aspirantes a determinadas plazas convocadas en régimen de concurso de méritos o en régimen de concurso/oposición.

La duración de los Cursos de Enseñanza abierta es de ciento veinte (120) horas y su valor académico es el de doce (12) créditos. El profesorado prepara los materiales didácticos que el alumno recibe y sobre los que trabaja por su cuenta. Con caracter optativo asiste a las sesiones presenciales a las que se les convoque que se celebran bien en la Sede Central, en Madrid, o en los Centros Asocisados repartidos por todo el territorio de las ahora Comunidades Autónomas en que se organiza administrativamente España. El Curso de Informática Jurídica se imparte en la UNED desde el año 1992.

Los contenidos del Curso de Informática Jurídica comprenden: introducción a las ciencias de la computación (incluídos sus fundamentos lógicos y matemáticos), el derecho como información y su tratamiento automatizado, sistema operativo, procesamiento de textos, bases de datos (arientadas estas cuestiones a las tareas del jurista), aparte de un segundo bloque de temas más específicamente jurídicos como son el tratamiento automatizado de los datos de caracter personal, la propiedad de los bienes informáticos, los llamados delitos informáticos y una iniciación a los contratos informáticos.

La evaluación del aprovechamiento del curso se hace sobre unos ejercicios que el alumno recibe y envía cumplimentados al equipo docente que los corrige. Suelen ser tres las evaluaciones llevadas a cabo y consisten cada una de ellas en una prueba objetiva, de selección de alternativas de respuesta, y en una prueba de ensayo, una redacción sobre algún tema del repertorio de los mismos que se les ofrece.

El título de este curso de Informática Jurídica se completa con el de otro curso que se llama "Informática y

Derecho: Derecho informático". Ambos podrían refundirse en la sola denominación de "Derecho informatizado y Derecho Informático", o aun separarse en "Derecho informatizado", por una parte (que giraría en torno a la informática jurídica de gestión, a la informática jurídica de documentación e investigación y a la informática jurídica aplicada a la docencia y a la evaluación), y en "Derecho informático", por otra.

Por lo que se refiere a la sistematización de los contenidos de un posible programa de "Derecho informatizado y Derecho informático" nuestra opinión o sugerencia es que habría que tratar de conseguir una estructura decimal, codificada y jeràrquica, partiendo naturalmente del sector 8 de nuestra clasificación radical de los saberes que se corresponde con el apartado dedicado a "Ciencia y Técnica"[7]. He aquí una primera propuesta, susceptible obviamente de correcciones y mejoras:

80: Informática:

Fundamentos electrónicos y matemáticos

81: Filosofía y Sociología de la informática y de la telemática
Planteamiento general: Informática y Derecho

82: Equipamiento informático y telemático
Máquinas y programas [virus y encriptación incluídos]
Sistemas operativos. Windows
Hojas de cálculo
Otros programas

83: Lenguaje e informática
Tesauros
Procesadores de textos
Linguística computacional
Bases de datos

84: Historia de la informática y de la telemática y su situación actual
Internet: navegadores, buscadores, etc.
Web

85: Enseñanza informatizada y de la informática
Programas de utilización educativa
Bases de datos educativas

Los epígrafes que siguen (86, 87 y 88) pertenecen ya al grupo del "Derecho informático" y nos ocuparemos de ellos en el apartado correspondiente.

5.- UNA NUEVA RAMA DEL DERECHO

Derecho Informático.

La aparición de un nuevo derecho fundamental o de la personalidad, de toda persona humana, como es el llamado derecho a la intimidad, privacidad de la información sobre uno mismo, o sobre la vida privada ensancha el horizonte de los constitucionalistas y civilistas. Lo mismo ocurre en el ámbito de los civilistas y mercantilistas

[7] Nuestra clasificación radical de los saberes (válida también para clasificar los libros de una biblioteca o los asuntos de una escribanía) quedó expuesta en una nota anterior. En la compartimentación del sector 8 (Ciencia y técnica) que se hace a continuación no es difícil reconocer cierta correspondencia entre ella y la clasificación primaria o de primer nivel, sobre todo en los apartados 81 (Filosofía), 84 (Historia), y 85 (Enseñanza).

respecto al nuevo concepto de la propiedad sobre bienes y productos informáticos, tales como la propiedad de los programas de ordenador y de las bases de datos. Los penalistas podrían ocuparse, como los sociólogos y criminalistas, de nuevos supuestos de conductas delictivas como es el caso de los llamados delitos informáticos. Los administrativistas, y aun los especialistas en Derecho tributario, podrían atraer para sí el estudio de las concesiones de explotación de servicios a los operadores de telefonía digital, a los proveedores de conexión a la red abierta de nodos de información que es Internet. Y de ahí en adelante.

¿Qué pasa con el Derecho de la minería, de la agricultura, de la educación o de la sanidad?. Que se han configurado o se van configurando como ramas autónomas del Derecho, desgajadas de la que, o de las que, eran una parte. No es cuestión pacífica, desde luego, esta de la autonomía, siquiera a efectos científicos y didácticos, de las nuevas disciplinas jurídicas. Hay que andar con tino para no crear miniespecialidades innecesarias, pero hay que ser generosos e imaginativos para no cerrar posibles caminos de desarrollo científico y social.

Por descontado que el Derecho es uno y que la hipercompartimentación de la Ciencia jurídica conlleva el riesgo de, como Minotauro en el laberinto, quedar encerrados en la sutileza de elucubraciones y distingos puramente conceptuales que han perdido el norte de la unidad de la justicia. No hay que trocear el Derecho hasta el extremo de que hagamos que desaparezca: ocurriría como si al enfermo, cansado de peregrinar de un especialista a otro, no se le considerase al fin como un ser completo que necesita al fin la atención de un generalista, o siquiera un planteamiento general de su situación como enfermo de una pieza.

Por fortuna nuestros estudiantes de primero de Derecho encuentran en el Derecho romano esa perspectiva unitaria deseable de la ciencia jurídica, con sus secciones de derecho procesal, de derechos reales, de derecho de familia y sucesiones, de derecho de obligaciones, etc. Se tiende hoy a los despachos de abogados integrados por especialistas diversos. Supongo que cuando les llegue un asunto, en una primera consideración, todos opinarán sobre el caso en cuestión antes de pasarlo a quienes, por su específica preparación, se hallen más relacionados con la materia a que en concreto se refiera; también es de suponer que, al final, si es preciso, el asunto volverá a pasar otra vez por una especie de instancia coordinadora para garantizar que no quedan cabos sueltos que resolver, para velar por la buena marcha del asunto en su totalidad.

Queremos decir que la Ciencia del Derecho es una, como es una la idea de Justicia, como debe ser global la comprensión de un caso práctico. Pero ello no contradice que, dentro del amplio marco de lo jurídico, se observen diferenciados campos específicos en orden a la legislación, en orden a la jurisprudencia, en orden a la docencia, en orden a la investigación y en orden a las publicaciones científicas. Uno de esos campos específicos, o áreas (como con la Ley española de Reforma Universitaria en la mano deben llamarse) es sin duda, en nuestra opinión y en la de otros muchos, el Derecho Informático.

Entendemos que el Derecho informático, como el Derecho agrario o como más recientemente el Bioderecho, no puede abordarse sin cierto conocimiento de la realidad sobre la que se asienta, la informática en este caso, la agricultura o la biología en los otros supuestos. Ocuparse de la normativa sobre firma digital sin una cierta información sobre mensajes cifrados que circulan por una red de nodos, o tratar de los aspectos jurídicos de la protección de datos personales digitalizados sin saber qué sea la información digitalizada, por poner sólo dos ejemplos, no parece que sea lo razonable.

Proponemos, por eso, el reconocimiento en nuestros planes de estudio del área de Derecho informático, con carácter de asignatura de contenidos propios. El volumen de normas legales y, aunque más modestamente, de sentencias jurisprudenciales, y desde luego la cantidad y el nivel científico de publicaciones periódicas y no periódicas, así como los programas de docencia que en España, en Europa y en el continente americano se están llevando a cabo desde hace ya bastantes años; (y, habría que añadir, la celebración de Congresos como el presente) avalan suficientemente la propuesta que aquí se defiende del reconocimiento de una nueva rama del Derecho que, perfilándola en sus justos límites, bien pudiera llamarse "Derecho informatizado y Derecho informático".

¿O acaso Ciber-derecho? ¿O informa-ius, infor-ius? Iuscibernética fue el título del primer libro del profesor Losano sobre la materia. Iurismática fue el nombre que empleamos en nuestro primer artículo sobre el tema. Posiblemente quedaría mejor así: "Ciberderecho: Derecho informatizado y Derecho informático".

Acerca de los contenidos deseables de un completo programa de "Derecho informatizado y Derecho informático" nos remitimos a lo dicho a propósito de "Informática Jurídica. Una experiencia docente" y a lo que diremos a continuación sobre "Informática y Derecho: Derecho informático. Una experiencia docente".

6.- "DERECHO INFORMATICO".

Una experiencia docente

El Curso de Informática y Derecho: Derecho informático se imparte en la UNED desde el año 1997.

Los contenidos del Curso de Derecho informático en el actual programa comprenden: La contratación por medios telemáticos, Datos personales informatizados, Prueba procesal y documento electrónico, Internet, Teletrabajo, Ilícitos de la Informática, Propiedad del Software, Régimen de las bases de datos, Telecomunicaciones, Firma digitalizada.

La evaluación del aprovechamiento del curso también se hace sobre unos ejercicios que el alumno recibe y envía cumplimentados al equipo docente que los corrige. Suelen ser también tres las evaluaciones llevadas a cabo y también consisten cada una de ellas en una prueba objetiva, de selección de alternativas de respuesta, y en una prueba de ensayo, una redacción sobre algún tema del repertorio de los mismos que se les ofrece.

Como continuación de lo dicho al tratar de la "Informática Jurídica", una experiencia docente, cabe completar aquí el índice sistemático allí iniciado. La clasificación que sigue comprende ya los contenidos de esta nueva rama del Derecho que es el Derecho informático[8].

86: *Bienes informáticos y*
Contratación informática [comercio electrónico]

87: Vida privada [datos nominativos] e
Ilícitos informáticos [derecho penal]

88: Otras ramas del Derecho informático
Ciberderecho laboral: Teletrabajo
Ciberderecho procesal: prueba procesal
Ciberderecho administrativo:
régimen jurídico co de las telecomunicaciones (Tel.)
régimen jurídico de los dominios (Dom.) etc.

Los epígrafes que acabamos de enunciar, como se puede observar, pertenecen ya al grupo del "Derecho informático". Se notará que, por mantenernos fiel a una primer nivel de estructura decimal omnicomprensiva, no ha habido más remedio que contar con un número de apartados de base; pero eso no es obstáculo para después derivar de ellos las oportunas subramificaciones. Llegados a este punto, se nos plantea la duda de si seguir la decimalización, codificada,o pasar directamente a la denominación, abreviada ciertamente, de las puntuales cuestiones: telecomunicaciones [abreviadamente, Tel], dominios [abreviadamente, Dom], etc.

Que los bienes informáticos y los contratos informáticos se agrupen bajo un sólo código, el núm. 86, tiene la lógica de que se trata de lo que podría decirse Derecho informático del patrimonio, algo que conecta con el actual planteamiento de una fusión, a efectos de código único, del derecho civil y mercantil.

Por lo que se refiere a la unificación, a efectos sólo de una clasificación sistemática decimal, de la protección de datos personales y los ilícitos penales informáticos, pensamos que se justifica desde el punto de vista de que en

[8] Inicialmente nos parecía que la sistemática de los contenidos de Derecho informático podía ser ésta: 81, Datos personales; 82, Prueba procesal; 83, Propiedad; 84, Contratos; 85, Delincuencia; 86, Teletrabajo; 87, Internet; 88, Telecomunicaciones; 89, Varios.

uno y en otro caso se alude a comportamientos que, por prohibidos (la invasión de la intimidad y cualquier otro comportamiento ilícito), conllevan una sanción.

El apartado 88 es residual y abarca todo lo que no se ha podido incluir en los apartados anteriores. El apartado 89, dedicado a Varios (otras técnicas y otras tecnologías), no es aprovechable para nuestros fines de sistematización de los contenidos de "Derecho Informatizado y Derecho informático".

7.- FUENTES DE DOCUMENTACION Y ASISTENCIA AL ALUMNO

Materiales para el estudio de Informática y Derecho

Cada uno de los Cursos de Enseñanza abierta cuenta con la correspondiente Guía didáctica que, junto con el material docente necesario, en nuestro caso un libro por curso, se remite al alumno.

El libro bàsico para el curso de Informática Jurídica, redactado por los profesores del Curso y editado por la UNED en su Colección Educación Permanante, lleva precisamente este título: Informática Jurídica. Es una obra de 296 págs que se inicia, como todas las de la colección, con un Prefacio, en el que se expone "la razón de ser del presente curso".

Se dice, entre otras cosas, en el Prefacio: "Como toda ciencia nueva la de la informática, está hecha de un lenguaje esotérico y balbuciente que es preciso fijar y comprender. Se trata de hacer asequible este lenguaje, de suministrar la correspondiente información de base que permita comprender más tarde las aplicaciones de la informática al tratamiento de la información jurídica".

Por lo que se refiere al Curso de Informática y Derecho: Derecho Informático, también se ha editado un libro que se titula del mismo modo y que pertenece a la Serie "Textos de Educación Permanente. Programa de Enseñanza Abierta".

Los contenidos de los libros son los mismos contenidos de los Cursos, a lo cual nos hemos referido ya antes. Mientras llega el momento de hacer nuevas ediciones de los libros, se envian a los alumnos, como material complementario, las oportunas "adendas" en las que se incluyen tanto explicaciones sobre temas no tratados en el correspondiente libro, como textos legislativos de aprobación más reciente: por ejemplo, sobre firma electrónica y comercio electrónico [con base en las nuevas normas de septiembre de 1999 y de febrero de 2000][9], y sobre la nueva Ley de Protección de Datos de diciembre del año pasado[10].

En ambos cursos se incluyen repertorios bibliográficos a fin de que el alumno pueda ampliar su información. La lectura y reseña de alguno de esos libros, normalmente a elección del alumno, puede ser objeto de alguna de las llamadas pruebas de ensayo.

Los alumnos de Enseñanza Abierta, como ocurre con los de Enseñanzas Regladas, tienen a su disposición un horario llamado "de atención tutorial", al menos una tarde por semana, en que pueden ponerse en contacto telefónico con el profesor para resolver cualquier duda o recibir aclaraciones sobre los contenidos de la materia en que esté matriculado.

Por otra parte, independientemente de este horario de atención personal al alumno, se suelen organizar conferencias en los Centros Asociados a las que asisten los alumnos pertenecientes a ese Centro y que son impartidas

---

[9] Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica (BOE 18 sept 1999). Orden [del Ministerio de Fomento] de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica (BOE 22 febr 2000).

[10] Ley Orgánica 15/1999, de 13 de diciembre (Jefatura del Estado), de Protección de Datos de carácter personal (BOE 14 dic 1999). En virtud de esta Ley queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

por los profesores del Curso. Las conferencias teóricas se pueden completar con sesiones de caracter práctico. Así se hace en nuestro caso.

Habrá que indicar ahora que nuestra Universidad a Distancia está tomando cada vez más el carácter de Universidad semipresencial, en cuanto que combina el estudio individual a distancia, fuera del aula, con la asistencia a conferencias, sesiones prácticas, videoconferencias y atención personalizada por parte del profesor-tutor de los Centros y aun de los profesores de la llama Sede Central, ubicada en Madrid.

8.- METODOS DE ENSEÑANZA Y DE EVALUACION

Un método semipresencial.

En la docencia del Ciberderecho, del Derecho Informático y del Derecho Informatizado, rigen en la UNED casi los mismos criterios que en las Enseñanzas Regladas, a saber: los materiales que se llaman autosuficientes, las *tutorías,* las ocasionales *sesiones presenciales,* las *pruebas de evaluación* (que en el caso de los cursos a que nos estamos refiriendo son exclusivamente a distancia, no presenciales).

Las tutorías.- Determinados días de la semana, y en horarios fijados de antemano y previamente divulgados, los alumnos pueden concectar con el profesor del Curso, generalmente por teléfono, o acudiendo personalmente a la Universidad. La relación profesor-alumno sirve para resolver problemas planteados, aclarar conceptos, dar orientaciones oportunas, ampliar información sobre material bibliográfico y motivar y estimular al alumno.

Además de las tutorías de presencia o por teléfono caben naturalmente la comunicación por correo electrónico o vía fax. Otra forma de comunicación con los alumnos se establece cuando el profesor les devuelve los ejercicicios corregidos y comentados. También en ese momento, el profesor puede emitir una enseñanza, una orientación oportuna que, en gran manera, servirá para que el alumno complete su aprendizaje y su formación.

Las sesiones colectivas presenciales.- Las sesiones que celebra el profesor o profesores con los alumnos qué opten por asistir a las mismas resultan muy útiles para explicar ciertas cuestiones y para realizar ciertas prácticas (manejo de un programa de procesamiento de textos, uso de bases documentales de información jurídica, sesiones de búsqueda de información por los servicios de Internet, etc.)

Estas sesiones presenciales presentan además la dimensión de "talleres" en los que se consigue desarrollar los hábitos de colaboración entre los participantes, por un lado, y comprobar, por otro, el verdadero nivel de rendimiento de los participantes.

La evaluación.- La enseñanza bien concebida debe contar desde el comienzo con unos buenos modos de evaluación de los aprendizajes: docencia y evaluación son dos caras de la misma moneda y deben concebirse en recíproca dependencia.

La enseñanza de Informática y Derecho se ha planificado incorporando pruebas de evaluación a los materiales didácticos,suministrando al alumno la información sobre la que luego han de versar las pruebas de evaluación y, en definitiva, estableciendo ciertos tipos de ejercicios que, de una parte, resulten muy claramente determinados "a priori", es decir, desde el mismo momento del comienzo de la tarea docente, y, de otra parte, sirvan a los objetivos que se persiguen con la enseñanza de esta nueva ciencia que tiene un contenido práctico, que se orienta a la acción: la acción de tratar la información y la acción de resolver un conflicto de intereses.

De dos tipos son las pruebas que deben realizar los alumnos: las objetivas o cerradas y las de tipo abierto o de ensayo.

Las pruebas objetivas empleadas en ambos cursos son las de selección de respuesta. Dada una serie de cuestiones o enunciados, con varias alternativas de respuesta (a, b, c) para cada uno, se trata de que el alumno encierre

dentro de un círculo la contestación que considere correcta. Es obvio que las otras posibles respuestas, los distractores, o sea, las alternativas de respuesta que no son correctas, debe ofrecer cierta dificultad de reconocimiento, es decir, deben ser aparentemente válidas. También es obvio que cuanto mayor sea el repertorio de cuestiones, y de alternativas de respuestas ofrecidas, más significativa resultará la prueba.

No haría falta decir que hay que evitar las preguntas irrelevantes en su contenido, de pura memorización de nombres y fechas o sobre cuestiones poco significativas en el ámbito de los conocimientos que se trata de evaluar. De hecho, de cada una de las tres partes de las que cada curso se componen, se hacen pruebas de 30 items, con tres alternativas de respuesta para cada item.

La corrección de cada una de estas pruebas es totalmente objetiva y puede realizarse mecánicamente, utilizando una lectura óptica de marcas. Se comprueba en cada item si la respuesta elegida por el alumno es exactamente la considerada como verdadera. Se contabiliza el número de aciertos y de errores y se aplica una fórmula de correción que suele ser ésta: total de aciertos menos una fracciòn en la que el numerador es el número de errores y el denominador el número de alternativas menos uno. La puntuación obtenida se convierte después a la escala que va de cero a diez, en el sistema que se usa en España, y se otorga la calificación correspondiente que se hace además constar en el ejercicio.

Las pruebas de ensayo, de redación o abiertas. Se suministran con el material de estudio un repertorio amplio de este tipo de pruebas a fin de que el alumno seleccione la que le interese. Van desde la redacción sobre algún tema que guarde relación con el contenido de los programas a que los cursos se refieren, hasta el comentario crítico de determinados textos legales, pasando por la reseña de alguno de los libros indicados en el repertorio bibliográfico, o la selección, denominación, sistematización y comentario crítico de noticias de prensa, artículos de revistas, decisiones jurisprudenciales o cualquier otra documentación relacionada con la informática, la informática jurídica o el derecho informático.

Para calificar las pruebas de ensayo se las analiza desde diversos puntos de vista, tales como los siguientes:

a) dominio y empleo de terminología adecuada, con corrección, claridad, precisión, sin vaguedades o consideraciones extravagantes.

b) capacidad para organizar la información de forma sistemática, destacando los elementos o apartados más importantes.

c) reelaboración personal, crítica y fundamentada de lo aprendido, no limitándose a la repetición memorística

d) originalidad, creatividad, imaginación cuando la respuesta se preste a ello.

e) calidad de la relación entre los conceptos: diferencias, semejanzas, causas, efectos, etc.

9.- CONCLUSIONES

1. El tratamiento automatizado de la información resulta ser, como escribió Frossini, la mayor novedad del último tercio de este siglo. Es un hecho que, junto al lenguaje humano, el hombre ha creado lo que se llama el lenguaje máquina, lo que, hasta cierto punto, le permite hacerse entender con los equipos informáticos. Sin duda que la información digitalizada está creando nuevos hábitos, nuevas necesidades, nuevas posibilidades y también, como un rebufo del progreso técnico, algunos nuevos problemas. El tratamiento industrial de la información significa para el jurista una herramienta que hay que aprender a usar y una actividad que hay que regular, que de alguna manera hay que reglamentar. Los profesionales del Derecho de nuestro tiempo no podemos desconocer las implicaciones existentes entre la Informática y el Derecho.

2. El Derecho es, entre otras cosas, información e información escrita. El lenguaje es elemento imprescindible del Derecho, la herramienta del jurista. El Derecho requiere de escritura y la escritura hoy pasa por las marcas digitales, por los octetos, y por el folio electrónico, por la videoescritura. El jurista escribano manual y aun el jurista mecanógrafo son ya más bien una reliquia del pasado.

3. Los programas procesadores de texto, sobre facilitar el hecho de la escritura, posibilitan la organización de las piezas de información que crea o que utiliza el jurista, contribuyen a fomentar su gusto por la armonía y el orden lógico, permiten la cooperación, el intercambio de información entre colegas. En el ámbito del Derecho, el tratamiento automatizado de la información hace posible una estética funcional, operativa, que potencia la eficacia de cualquier documento.

4. Con los programas de gestión de bases de datos documentales la recuperación de documentos jurídicos, esto es, de unidades de información jurídica, puede hacerse al instante y con toda garantía. La recuperación de piezas de información jurídica en una base de datos se debe poder hacer tanto en modo de búsqueda por palabras controladas, organizadas, de un Tesauro como por el modo de búsqueda del llamado texto libre o sin estructurar.

   Un Tesauro jurídico que comprenda un exhaustivo y bien sistematizado repertorio de términos constituye para el jurista un valioso elemento de consulta y aun de formación. Si no existiese un buen Tesauro jurídico habría que crearlo. Si existiese, habría que actualizarlo periódicamente, por especialidades o áreas de conocimiento..

5. En la Universidad Nacional de Educación a Distancia, de España, con sede central en Madrid, y dentro de las llamadas Enseñanzas No Regladas (que dependen del Vicerrectorado de Educación Permanente) se imparte anualmente, desde el año 1992, un curso de Informática Jurídica. Este curso está dentro del Programa de Enseñanza Abierta y pueden inscribirse en él cuantos deseen. Sus destinatarios naturales, por así decirlo, son estudiantes y profesionales de derecho y también, porque no se exigen especiales requisitos para seguirlo, empleados de la administración de justicia o de las administraciones públicas, entre otros. El curso tiene la duración de un año académico aproximadamente y, superadas las correspondientes pruebas de evaluación a distancia, da derecho a un Diploma oficial de la Universidad por valor de 12 créditos, correspondientes a 120 horas lectivas.

   El curso de Informática Jurídica que se sigue en la UNED , desde el año 1992, incluye entre sus contenidos los temas de: fundamentos del tratamiento automatizado de la información, sistemas operativos, programas procesadores de texto, programas de gestión bases de datos y bases de datos jurídicas, régimen legal de protección de datos de carácter personal, derecho de propiedad sobre bienes informáticos, iniciación a los llamados delitos informáticos, iniciación a los contratos informáticos, etc.

6. Siendo deseable no perder de vista la perspectiva unitaria del Derecho, es lo cierto que la ciencia del Derecho aparece compartimentada en campos de especialidades y areas de estudio.

   Por lo específico de las normas legales que lo conforman, del área de docencia en la que se imparte y de las publicaciones científicas y Congresos de que está siendo objeto, el Derecho informático se configura como una rama del Derecho, con contenido y método propios, que debe tener el oportuno reconocimiento legal en los planes de estudio de la Licenciatura de Derecho y también en otros planes de estudio, así en los de la Escuela Técnica Superior de Ingenieros Informáticos y en los de la Escuela Técnica de Ingenieros Informáticos, dada las implicaciones jurídicas de la actividad profesional de los que se formen en tales Escuelas.

   La Informática Jurídica, como realidad sobre la que el Derecho Informático se construye, debe ser *incorporada al área de conocimientos que bien podría designarse con el nombre de "Derecho informático y Derecho Informatizado".*

7. Desde 1997 se imparte cada año en la UNED un curso de "Informática y Derecho: Derecho Informático" que comprende los temas de: Bienes informáticos (incluída la propiedad de los programas de ordenador; la propiedad de las bases de datos y de los productos multimedia; el régimen jurídico de las topografías de semiconductores); Contratos informáticos y comercio electrónico; Datos nominativos y su protección legal; Derecho informático penal: los llamados delitos informáticos; Teletrabajo; Prueba procesal y documento electrónico; Régimen jurídico de las telecomunicaciones; Internet; etc. Los requerimientos, duración del curso, características de las pruebas y título obtenido son idénticos a los señalados para el Curso de Informática Jurídica, pertenecientes ambos al Programa de Enseñanza Abierta de las Enseñanzas No Regladas de la UNED.

8. La docencia de los cursos de "Informática Jurídica" y de "Informática y Derecho: Derecho Informático" en la UNED se está llevando a cabo con ayuda de las oportunas Guías didácticas y los libros básicos, como materiales docentes que la propia Universidad pone a disposición de los alumnos. Como apoyo de la docencia se cuenta con tutorías, esto es asistencia personalizada al alumno, con sesiones colectivas presenciales, con videoconferencias y en un futuro muy próximo con los oportunos sitios Web.

   La evaluación de estos cursos sobre Informática y Derecho, en la UNED, se realiza mediante pruebas a distancia tanto objetivas, cerradas, como de ensayo, abiertas. En estas últimas se tienen en cuenta la precisión terminológica, la capacidad de sistematización de los contenidos de la exposición, el sentido crítico, la creatividad y la interrelación de conocimientos.

9. ¿Qué es lo que queda en limpio de las presentes consideraciones en torno a la "Enseñanza del Derecho Informático y del Derecho Informatizado en la UNED"?. Decía d'Ors, filósofo español del siglo pasado: "una sóla cosa te será contada y es la obra bien hecha". La obra bien hecha como aspiración muy noble del ser humano. La obra bien hecha como emblema de un comportamiento ético y cabal. La obra bien hecha como paradigma de la felicidad interior, del autologro, de la autorrealización generosa, difusiva y solidaria. Sin duda que la Informática puede ser una aliada de lo obra bien hecha. Pero hay que andar con cautela.

Los avances de las "nuevas tecnologías" son como pasos de gigante. Y el ser humano quizás pierda con ellos el sosiego de los pasos serenos y en compañía. Las sucesivas, *aceleradas conquistas* de la ingeniería informática pueden producir en los usuarios de sus productos el desasosiego natural de quien siempre va a la zaga (de los inventos y de los demás). *Ése es, a nuestro parecer, uno de los males de la cultura del ordenador: la sensación de provisionalidad y el suplicio tantálico de "nunca estar llegados y siempre estar llegando", parodiando la expresión de un poema.* Aparece la sensación de quedarse atrás, de no estar "a la última" precisamente sino desfasado y obsoleto como un viejo trasto al que ya nadie quiere, que para nada sirve.

No cabe duda de que con el ordenador, y en general con la informática, se pueden realizar *tareas muy atractivas y útiles* en el ámbito del Derecho: se puede prestar un mejor servicio a los demás. No es discutible que la nueva rama del Derecho informático acabará por abrirse paso entre la rutina, la resistencia al cambio y los intereses encontrados. Ojalá que nuestra sociedad de la información automatizada resuelva con acierto los retos que el tratamiento industrial de la información plantea: con buenas leyes, con buenos programas de enseñanza, con buenos profesionales, que ésa es la base de todo.

Sólo expreso, para terminar, *una preocupación: el temor de que rindamos indebido culto a las máquinas de trabajar y al trabajo,* que estos instrumentos nos oculten la visión de la realidad de los seres humanos que, nuestros próximos y nosotros mismos, somos. Tal vez, entre documento y documento bajados de la red, habría que encontrar tiempo (el que ganamos con el uso de la máquina) para, sin avaricia, emplearlo sabiamente en, por ejemplo, cuidar del jardín, pasear, leer un poema, respetar la sobremesa en familia o conversarse amistosamente una bebida en humana compañía: dando primacía a lo que realmente la tiene, una vida verdaderamente humana, más libre y plena gracias al buen servicio de las subordinadas máquinas.

VII CONGRESO IBEROAMERICANO DE DERECHO E INFORMATICA
PROGRAMA

Lunes 24 de Abril de 2000

17 :00 -19 :00 Tema 1: DERECHO E INTERNET EN EL NUEVO MILENIO

Expositor:	***Dr. Emilio Suñé Llinás***	(España)		
Panel:	Dr. Humberto Carrasco Blanc	(Chile)	Dr. Ruben Ugarteche V.	(Perú)
	Dr. Juan Rodriguez Alvarez	(España)	Dr. Ezequiel Zabale	(Argentina)
	Dr. Julio Núñez Ponce	(Perú)		
Coordinador:	Dr. Carlos Ferreyros Soto	(Perú)		

19 :00 Inaguración

20 :00- 22 :00 Tema 1: DERECHO E INTERNET EN EL NUEVO MILENIO

Expositor:	***Dr. Audilio Gonzales Aguilar***	(Francia)		
Panel:	Dra. Marina Vargas Gomez U.	(España)	Dra. Beatriz Rodriguez A	(Uruguay)
	Dr. Luis Alfonso Muñoz Najar	(Perú)	Dr. Marcelo Huerta	(Chile)
	Sr. Erick Iriarte Ahon	(Perú)		
Coordinador :	Dr. Carlos Ferreyros Soto	(Perú)		

Martes 25 de Abril de 2000

9 :00- 11:00	Comisiones Aula Magna A	Coordinador Dr. Aldo Elliot	(Perú)
11:00-13 :00	Comisiones Aula Magna A	Coordinador Dr. Diego Suárez	(Argentina)

Tema 1: DERECHO E INTERNET EN EL NUEVO MILENIO

17 :00- 19 :00 Tema 2: NUEVOS DESAFIOS AL DERECHO INFORMATICO EN EL NUEVO MILENIO

Expositor:	***Dr. Daniel Ricardo Altmark***	(Argentina)		
Panel:	Dra. María José Viega Rodriguez	(Uruguay)	Dr. José Espinoza C.	(Perú)
	Dr. Juan José Paez	(Ecuador)	Dr. Pedro Juez Martel	(España)
	Dr. Fernando Martins Castro	(Brasil)		
Coordinador:	Dr. Julio Núñez Ponce	(Perú)		

19 :00- 21 :00 Tema 2 : NUEVOS DESAFIOS AL DERECHO INFORMATICO EN EL NUEVO MILENIO

Expositor:	***Dr. Julio Tellez Valdez***	(México)		
Panel:	Dr. Audilio Gonzales Aguilar	(Francia)	Dr. Aldo Elliot Segura	(Perú)
	Dra. María Eugenia Gayo	(España)	Dr. Martin Moscoso V.	(Perú)
Coordinador:	Dr. Julio Núñez Ponce	(Perú)		

Miércoles 26 de Abril de 2000

9 :00- 11 :00	Comisiones Aula Magna A	Coordinador Dr. José Espinoza Céspedes	(Perú)
11 :00- 13 :00	Comisiones Aula Magna A	Coordinador Dr. Francisco Eugenio Díaz	(España)

Tema 2 : NUEVOS DESAFIOS AL DERECHO INFORMATICO

15 :00- 18 :00 Tema 3: NUEVOS ENFOQUES DE LA INFORMATICA JURIDICA Y DE LOS SISTEMAS APLICADOS AL DERECHO

Expositores:	***Dra. Yarina Amoroso***	(Cuba)	Dr. Marcelo Bauzá Reilly	(Uruguay)
Panel:	Dr. Cristian Hess Araya	(Costa Rica)	Dr. Oscar Gómez	(Perú)
	Dra. Patricia Reyes	(Chile)	Dr. José Francisco Salas	(Costa Rica)
	Dr. Rodrigo Obrador	(Chile)		
Coordinador:	Dr. Carlos Ferreyros Soto	(Perú)		

Jueves 27 de Abril de 2000

- Exhibiciones de Sistemas aplicados al Derecho Temas 3 y 4 Aula Magna B

9 :00-45 :00	Sistema de Información Jurídico LEGIS	(Chile)
9 :45-10 :30	Sistema Costaricense de Información Jurídica	(Costa Rica)
10:30 –11:00	Exhibición de Sistema de CETID	(Ecuador)
11 :00- 12 :00	Sistemas aplicados al Derecho del Ministerio de Justicia	(Perú)
12 :00- 12:30	Exhibición de Sistema Experto de Dr. Jayme Cavalcanty	(Brasil)
12:30-13:00	Sistema INFORJU Dr. F. Doberti	(Perú)

17 :00- 19 :00 Tema 4: MODERNIZACION DEL ESTADO E INFORMATICA

Expositor:	***Dr. Juan Diego Castro***	(Costa Rica)		
Panel	Dr. José Vicente Cebrian	(España)	Dr. Héctor María Chayer	(Argentina)
	Dr. José María Alvarez Cienfuegos	(España)	Dra. Rocío Rondinel	(Perú)
	Dr. Pedro Patrón Bedoya	(Perú)		
Coordinador:	Dr. Valentín Carrascosa López	(España)		

19 :00-21 :00 Tema 4: MODERNIZACION DEL ESTADO E INFORMATICA

Expositor:	***Dr. Diego Suárez***	(Argentina)		
Panel:	Dr. Francisco Monterde Ferrer	(España)	Dr. Jesús Manuel Saez C.	(España)
	Dr. Fernando Arrunategui	(Perú)	Dra. Carmen Velarde	(Perú)
	Dr. Rodolfo Herrera Bravo	(Chile)		
Coordinador:	Dr. Carlos Ferreyros Soto	(Perú)		

21 :00- 22 :00 Tema 4: MODERNIZACION DEL ESTADO E INFORMATICA

Expositor : ***Dr. Carlos Ferreyros Soto*** (Perú) en representación del Dr. Carlos Torres y Torres Lara (Perú)

Viernes 28 de Abril de 2000

9 :00- 10 :00 : Comisión Tema 5 Aula Magna B

10 :00- 11 30: Comisión Tema 6 Aula Magna B Ponencia de Dr. Francisco Eugenio Díaz

11 :30- 13 :00 *Comisión Temas Varios Aula Magna B*

Coordinadora: Dra. Teresa Vargas

---

17 :00-19 :00 Tema 5: DERECHO EMPRESARIAL E INFORMATICA

Expositor:	***Dr. Juan Antonio Rangel Charles***	(México)		
Panel:	Dr. Ricardo Maguiña Pardo	(Perú)	Dr. Hector Peñaranda Q.	(Venezuela)
	Sr. Italo Fernandez Orrigi	(Perú)	Dr. Alberto Stewart B.	(Perú)
Coordinador:	Dr. Julio Tellez Valdez	(México)		

---

19 :00- 20 :00 Tema : Tecnología y Derecho : Un Caso aplicado a negocios.

Expositor: ***Ing. Richard Wadsworth Delgado*** – TELEFONICA SERVICIOS DIGITALES (Perú)

---

20 :00- 22 :00 Tema 5: DERECHO EMPRESARIAL INFORMATICO EN INTERNET:USO DE LA MICROFORMA DIGITAL

Expositor:	***Dr. Julio Núñez Ponce***	(Perú)		
Panel:	Ing. Guillermo Checa	(Perú)	Dr. Daniel Ricardo A.	(Argentina)
	Dr. Emilio Suñé Llinás	(España)	Dr. José Ochoa Reyes	(Perú)
Coordinadora:	Dra: Yarina Amoroso	(Cuba)		

Sábado 29 de Abril de 2000

9.:00-10:00 Tema 6 : UNIVERSIDAD, DERECHO E INFORMATICA

Expositor:	***Dr. Valentín Carrascosa López***	(España)		
Panel:	Dr. Francisco Eugenio Díaz	(España)	Dr. Julio Núñez Ponce	(Perú)
	Dr. Juan Rangel Charles	(México)	Dr. Marcelo Bauzá Reilly	(Uruguay)

---

11 :00-12 :45 *Tema 6 : UNIVERSIDAD, DERECHO E INFORMATICA*

Expositor:	***Dra. Teresa Vargas Osorno***	(Colombia)		
Panel:	Dr. Julio Tellez Valdez	(México)	Dra. Rocío Rondinel	(Perú)
	Dr. Guillermo Beltramone	(Argentina)	Dra. Katherine Fudinaga H.	(Perú)
	Dr. Jaime Lara	(Perú)		
Coordinador:	Dr. Juan Diego Castro	(Costa Rica)		

12:45 CLAUSURA

UNIVERSIDAD DE LIMA
BIBLIOTECA
115842
348.53
D3
14/05