Universidad de Lima
Escuela de Posgrado
Maestría en Derecho Empresarial

EN BÚSQUEDA DEL EQUILIBRIO ENTRE LA PROTECCIÓN DE DATOS PERSONALES, EL DEBER DE TRANSPARENCIA Y EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

Trabajo de investigación para optar el Grado Académico de Maestro en ´
Derecho Empresarial

Mariafernanda Rivera Prado

Código 20187019

Asesor

Desirée Bianca Orsini Wisotzki

Lima – Perú

Octubre de 2022

UNIVERSIDAD DE LIMA
SCIENTIA ET PRAXIS

IN SEARCH OF A BALANCE BETWEEN THE PROTECTION OF PERSONAL DATA, TRANSPARENCY AND THE RIGHT OF ACCESS TO PUBLIC INFORMATION

TABLA DE CONTENIDO

RESUMEN

Cada país que ha desarrollado un conjunto de derechos de protección de datos personales y de acceso a la información pública, lo ha hecho atendiendo a necesidades específicas, según su propio contexto socio-histórico cultural y Perú no es la excepción. Para entender cabalmente la protección de estos derechos y determinar los criterios con los cuales se garantice un equilibrio suficiente entre ellos, necesariamente tenemos que volver en el tiempo y observar la razón por la que éstos surgieron en Europa, Estados Unidos de Norteamérica y América Latina.

Entender el origen de estos derechos a partir de su contexto histórico nos permitirá determinar si es que el legislador peruano ha implementado la norma sobre protección de datos personales en coherencia con su realidad y necesidades; y si es que las autoridades competentes en Perú dirimen correctamente los casos en los que se contraponen los derechos contenidos en la Ley de Transparencia y Acceso a la Información Pública y el derecho a la protección de los datos personales.

A partir de un análisis concienzudo de lo antes expuesto, la presente investigación propondrá los criterios que deberá aplicar la autoridad competente para deliberar la controversia referida y procurar, así, un equilibrio razonable en la protección o limitación de estos derechos.

Palabras clave: derecho de protección de datos personales, *"a man´s house as his castle",* "*the right to be let alone*", Cambridge Analytica, derecho de acceso a la información, derecho al olvido, test de ponderación de derechos, la fórmula del peso.

ABSTRACT

Each country that has developed a set of personal data protection rights and access to public information has done so by addressing specific needs, according to its own socio-historical cultural context; and Peru is no exception. To fully understand the protection of these rights and determine the criteria with which a sufficient balance between them is guaranteed, we necessarily have to go back in time and observe the reason why they emerged in Europe, the United States of America and Latin America.

Understanding the origin of these rights from their historical context will allow us to determine if the Peruvian legislator has implemented the norm on the protection of personal data in coherence with their reality and needs; and if the authorities in Peru correctly settle the cases in which the rights contained in the Law of Transparency and Access to Public Information and the right to the protection of personal data conflict.

Based on a thorough analysis of the above, this investigation will propose the criteria that the competent authority must apply to deliberate on the aforementioned controversy and thus seek a reasonable balance in the protection or limitation of these rights.

Keywords: data protection, *"a man´s house as his castle",* "*the right to be let alone*", Cambridge Analytica, right of access to information, right to be forgotten, balancing test, the weight formula.

INTRODUCCIÓN

Estamos viviendo la cuarta revolución industrial, cuyas tecnologías llegan incluso a fusionar el mundo físico, biológico y digital. Desde luego, estos adelantos, provocan la aceleración de la velocidad a la que fluye la información de un punto geográfico a otro, haciendo relativas las distancias, tienen un impacto significativo en la economía, en general, en la industria, en específico; y también lo tiene, desde luego, en la forma de vida de las personas, influyendo en nuestra realidad más inmediata.

Con el internet, los celulares y las bases de datos, minuto a minuto se vienen creado y almacenado datos de manera masiva, al punto de afirmar que los datos son un recurso más valioso que el petróleo (Kershner, 2021). Sin embargo, a diferencia del petróleo, los datos por sí solos no son útiles ni tienen valor, es por ello que estas nuevas tecnologías tienen como objetivo tamizar ese universo de datos existentes para quedarse con aquellos que tengan calidad, valor y que proporcionen información relevante. La única herramienta que puede encontrar el "dato de oro" dentro de esa masa gigante de variados tipos de datos y a una velocidad apremiante es la tecnología misma, denominada Inteligencia Artificial (SANTILLÁN VÁSQUEZ, 2018, pp. 229–240). Si bien no existe definición unívoca sobre Inteligencia Artificial, podemos decir que esta es una disciplina científica que se ocupa de crear programas informáticos y construir máquinas que ejecutan operaciones similares a la cognición, inteligencia y comportamiento humano, teniendo algoritmos que permiten aprender (de manera automática) a partir de los datos que le son suministrados y así producir conocimiento exclusivo en base a ellos. (RUSSELL & NORVING, 2015, pp. 1–5)

Dado que en esta era, los consumidores están constantemente conectados a diversas plataformas y aplicaciones, exigen al mercado la oferta de productos cada vez más personalizados; las empresas requieren de datos para satisfacer esta necesidad, en base a los cuales puedan obtener información relevante de sus usuarios y ofrecer bienes y servicios innovadores, así como nuevas y mejores experiencias de consumo. Como consecuencia, podemos afirmar que solo aquellas empresas que cuenten con modelos de negocios basados en el tratamiento de datos y con la tecnología necesaria para procesarlos, lograrán un crecimiento sostenido en el tiempo.

La existencia de diversos sujetos (consumidores, proveedores, fabricantes y de las propias entidades de la administración pública, entre otros) que crean, alimentan y se benefician del tratamiento de bases de datos, ha obligado a los gobiernos a implementar medidas de protección para la información de sus ciudadanos. Dichas medidas han ido surgiendo en cada país en contextos históricos diferentes, lo que explica su diferente nivel de rigor. Así, mientras los países que integran la Unión Europea han impuesto medidas muy estrictas en un esfuerzo por proteger al ciudadano frente al (mal) uso que de sus datos puedan hacer las entidades gubernamentales, en los Estados Unidos de Norteamérica, solo el estado de California cuenta con un cuerpo normativo que restringe el uso de datos personales. La jurisprudencia a nivel federal tradicionalmente ha sido más bien cuidadosa en no restringir demasiado el derecho a la información de los ciudadanos, derecho cuyo ejercicio es considerado fundamental para el buen funcionamiento del sistema democrático.

Por otro lado, los países de América Latina tuvieron en su mayoría gobiernos dictatoriales hasta entrada la década de 1980. Ello originó que, una vez recuperada la democracia se implementaron prioritariamente normas de transparencia que permitieran a los ciudadanos obtener información sobre lo sucedido durante las dictaduras. Por otra parte, los escándalos de corrupción que se dieron durante los mismos años de regímenes autoritarios acrecentaron la necesidad de profundizar la protección de dichas normas y crear herramientas efectivas que permitiesen supervisar más efectivamente la gestión pública.

En el Perú este último problema, el de la corrupción ha venido ganando más relevancia con el paso del tiempo; lejos de disminuir, se ha incrementado aún a través de la democracia endeble. En febrero de 2022, la Defensoría del Pueblo de Perú presentó la quinta entrega de los Mapas de la corrupción en el Perú, documento en el cual se advierte que existen 27,275 casos de corrupción que se encuentran en trámite entre el periodo 2017 – 2020, detallando que por cada mil habitantes se dan 27 casos de corrupción. (Defensoría del Pueblo, 2022)

Lo aquí expuesto explica que gobiernos como el peruano no solo deban proteger los datos personales de sus ciudadanos, sino que también deban garantizar, sin limitaciones

injustificadas, su derecho a acceder a información de interés público. La trasparencia es claramente un elemento clave en el combate contra la corrupción; la gestión de los funcionarios públicos, parte importante a ser transparentada en beneficio de todos los peruanos.

Siguiendo el ejemplo de rigor europeo, el Perú, lo mismo que otros países de la región, ha implementado normas de protección de datos personales ciertamente estrictas. Ello ha derivado pronto en ciertos problemas, dado que los esfuerzos por transparentar los actos de la gestión pública, varias veces, se han visto enfrentados a las políticas de protección de datos personales, lo que hace bastante difícil dar con un equilibrio. La cuestión de procurar balance entre el derecho de protección de datos personales y el derecho de acceso a la información de interés público reviste, por lo tanto, especial vigencia.

La presente investigación consiste en un análisis de la forma en que las autoridades competentes dirimen este tipo de controversias y aplican normas en busca del mencionado equilibrio. En ese contexto, discutiremos también hasta qué punto y dentro de qué parámetros, derechos reconocidos por la jurisprudencia europea, como por ejemplo el derecho al olvido, pueden ser adoptados en nuestro ordenamiento y adaptados para funcionar efectivamente.

Luego de la revisión de esta problemática, proponemos, en esta investigación, un conjunto de criterios a ser aplicados por la autoridad competente para dirimir los casos en los que el derecho al acceso a la información pública se contraponga al derecho de protección de datos personales.

CAPÍTULO I

DIFERENCIA EN EL ORIGEN Y EVOLUCIÓN DE LA NORMATIVA SOBRE PROTECCIÓN DE DATOS PERSONALES EN EUROPA, ESTADOS UNIDOS Y LATINOAMÉRICA

1.1. Origen de las normas de protección de datos personales en Europa

Nuestra especie opera en la realidad, se adapta a la naturaleza, a los fenómenos, y adapta estos también a sus instituciones, a través del manejo de información. Es así que, en determinado punto, la necesidad de recopilar masivamente diferentes tipos de datos, cobra especial relevancia. A partir de dichos datos, de su procesamiento, los hombres toman decisiones y gestionan lo mejor que pueden el funcionamiento de diferentes aspectos de su vida diaria, en los más diversos ámbitos: agricultura, comercio, salud, educación, etcétera.

El valor del manejo sistemático de datos fue muy apreciado por Adolf Hitler, por ejemplo. Desde el inicio del régimen nazi en 1933, la información organizada fue empleada de forma estratégica para la manipulación de la ciudadanía, así como, por supuesto, para anticipar movimientos de oposición entre la población y fuera, en materia de política internacional. Ya en la Segunda Guerra Mundial, el manejo de sistemas de información fue clave en la carrera armamentista hasta 1945.

Durante el Tercer Reich los derechos civiles de los ciudadanos alemanes fueron suspendidos, fue restringida la libertad de expresión y, con el ideal de establecer una "sociedad ideal nazi"; las políticas del gobierno del Partido Nacional Socialista apuntaban directamente a la deportación, distribución en *ghettos* y, luego, a campos de concentración y exterminio, a todos los judíos que radicaban en Alemania. Para llevar a cabo tales objetivos, los nazis necesitaban identificar a cada uno de los judíos y sus ascendientes en territorio nacional. Hitler, entonces, empezó por realizar un censo general. En tales épocas, durante la década de 1930, un proceso de este tipo bien podía tomar a veces entre tres a cinco años, pues la tabulación de datos se realizaba

manualmente, entonces los nazis utilizaron nueva tecnología para el procesamiento de una cantidad masiva de datos en el menor tiempo posible. Dehomag (*Deutsche Hollerith Maschinen GmbH*), sucursal en Alemania de la empresa americana IBM (International Business Machines) fue quien facilitó estos procesos. La solución de Dehomag e IBM se basaba en el uso de tarjetas perforadas y máquinas clasificadoras D-II Hollerith: primeros tabuladores de clave, cuyos resultados fueron efectivamente muy aprovechables.

Las máquinas clasificadoras D-II Hollerith de IBM fueron contratadas por el gobierno alemán y lograron procesar 450,000 tarjetas perforadas diariamente, obteniendo como resultados de hasta 41 millones de personas en Prusia, el estado más grande de Alemania, en tan solo cuatro meses. El primer censo ordenado por Hitler fue realizado por civiles que fueron específicamente escogidos por tener una "mentalidad nacionalista" y que eran acompañadas por oficiales de la SS (*Schutzstaffel*), por lo que los censados se veían presionados a responder las preguntas que ayudasen a los nazis a identificar a las personas de origen ario y a las de origen judío. Las preguntas y datos que recolectaban los censistas estaban referidas a la siguiente información de los entrevistados partían de la nacionalidad, su domicilio, género, edad, religión, su primera lengua o lengua materna, cuantos hijos tienen, a que se dedican y en donde trabajan. Al identificar a un judío, el censador tenía orden expresa de marcar esa tarjera como una tarjeta especial de recuento para un judío en la parte correspondiente al registro del lugar de nacimiento, las tarjetas que tenían esta marcación especial eran procesadas separadas de las demás.

Figura 1
Fotografía de la máquina clasificadora de tarjetas de IBM en exhibición en el Museo del Holocausto de los Estados Unidos.
Tomada de (Frank Walker, 2017)

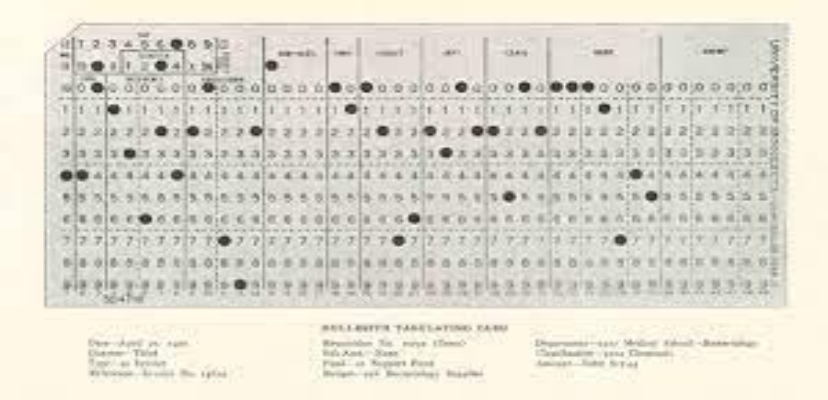

Figura 2
Imagen de Tarjeta perforada de IBM (Hollerith Tabulating Card)
Tomada de (University of Minnesota, 2018)

La tecnología de IBM permitió a la Oficina de Estadística del Reich tener información suficiente para disponerse a la promulgación de leyes y decretos antisemitas más efectivos. Las restricciones contra los judíos, que les impedían ejercer derechos laborales básicos, crear negocios, y acceder a servicios de salud y educación, cundieron.

Las tarjetas perforadas y las máquinas clasificadoras D-II Hollerith no sólo estaban a disposición de las oficinas gubernamentales del Reich, sino también a disposición de iglesias, bancos, empresas eléctricas, fábricas de automóviles, manufactureras y diversas empresas de diferentes rubros, por lo que Hitler se propuso organizar y administrar toda la información de judíos proveniente de todos estos canales de información valiosa. Es así que, mientras más clientes tenía Dehomag en Europa, más información estaba a disposición del Reich, que a través de sus departamentos dedicados a la ciencia racial o de investigación sobre familia, podían administrar: comparar y contrastar información de los judíos, referida inclusive a su vida privada, para intervenir en sus ingresos por planilla, ahorros, finanzas, horarios, lugar de trabajo, uso de productos, medicamentos, enfermedades, etc.

La ayuda de IBM a la Alemania nazi continuó incluso cuando ya se tenía conocimiento de la existencia de los campos de concentración y del quebrantamiento de los derechos amparados en normativas fundamentales que se daba en la época; a pesar de un declarado rechazo por parte del gobierno americano hacia el régimen de Hitler, que impedía a IBM seguir exportando tarjetas perforadas y repuestos de máquinas

clasificadoras a Alemania, la empresa se encargó de que todo este material ingresara a Alemania a través de otros países de Europa.

Así, en 1937, la tecnología de IBM era fundamental para la estrategia racial y de guerra de Alemania. El Departamento de Economía Militar del Ministerio de Guerra del Reich (*Mashinelles Berichtwesen*) y la Oficina de Información Automatizada estaban dedicadas a la "tecnología de las tarjetas perforadas"; contaban con todos los datos que provenían de las máquinas clasificadoras en la Gran Alemania, les permitía trabajar coordinadamente, con un mejor control sobre diferentes aspectos de la vida diaria de los alemanes y, claro, también de los judíos. Esta tecnología era utilizada además para efectuar censos en cada nuevo país invadido por los nazis durante la Segunda Guerra Mundial, y sus resultados podían estar listos en tiempos récord de hasta 48 horas.

Para 1939, Dehomag de IBM tenía máquinas dentro de los mismos campos de concentración, casi todos estos campos tenían un departamento especial para Dehomag conocido como el *Hollerith Abteilung*, centros estadísticos con detalles de análisis demográficos, asignaciones laborales diarias y tasa de subsistencia de sus rehenes. Durante la guerra estas máquinas permitían al gobierno alemán contar con información personal de cada obrero, oficial y soldado nazi, controlar las planillas de pago, las fábricas de municiones incluso podían permitirse tener un "registro de todos los comunistas y nazis". La recolección de todos estos datos, y su tratamiento permitía al gobierno nazi, distribuir dentro de la Alemania ocupada a obreros calificados, obreros reclutados o esclavos provenientes de otros países ocupados. Por ejemplo, si un oficial nazi necesitaba colocar en Polonia a una cantidad de técnicos que hablaran polaco sin ser polacos, era posible conseguir sus nombres y lugar de residencia exactos. La tecnología de IBM permitía a los nazis rastrear personas, registrar caballos y ganado que fueron confiscados por ellos en los países ocupados, les permitía tener registros de materiales, armas, ropa, repuestos, petróleo, caucho, acero, hiero, autos, camiones, registro de vuelos militares, heridas de guerra, ordenes de combate, balas, movimientos de tropas, etc. Cada uno de los registros necesariamente requería un diseño específico de tarjeta, cada una de las series de tarjetas perforadas llevaba su propia configuración según el propósito del registro de datos, por lo que se podían tener edificios enteros llenos de tarjetas perforadas. Esto resultó en un negocio muy lucrativo para IMB, como propietario de la patente, la técnica y los materiales específicos para producir estas tarjetas perforadas y que sólo

podían ser leídas por sus propias máquinas clasificadoras; por lo tanto, los nazis se vieron obligados a contratar sólo con IBM y no con otras empresas que pretendían y podían, ciertamente, brindar un servicio similar. (Black, 2001, pp. 66–102)

Una vez culminada la Segunda Guerra Mundial, y al conocer todos los delitos cometidos por los nazis, fue fundada la Organización de las Naciones Unidas y se celebró la Declaración Universal de los Derechos Humanos, con lo que la comunidad internacional buscó evitar, en lo sucesivo, se dieran atrocidades como las cometidas por los nazis, a través de un sistema de derechos internacional.

Tras los juicios de Núremberg, llevados a cabo por el Tribunal Militar Internacional, con el que por primera vez en la historia del mundo se autorizó a un tribunal internacional a responsabilizar personalmente a los principales representantes de un Estado por crímenes de derecho internacional, se hicieron públicos innumerables testimonios de las víctimas sobrevivientes del holocausto y el mundo pudo conocer cómo es que los nazis recopilaban y traban datos para cometer crímenes.

Es en este contexto que la Europa de post guerra estaba urgida de proteger el derecho de privacidad y de los datos de las personas; pero no fue sino hasta 1981, con el Convenio 108 – Consejo de Europa, que se rigió expresamente la protección en materia de tratamiento de datos personales. Esta es la primera norma internacional de carácter vinculante que protege a la persona contra los abusos que se puedan cometer en la recopilación y procesamiento de datos personales y brinda definiciones como las de fichero, tratamiento automatizado, autoridad controladora del fichero, categorías de información personal en relación de la sensibilidad del titular, obligación de adoptar medidas de seguridad, sanciones y flujo transfronterizo de datos personales. Luego de esto, la Unión Europea ha ido implementando una serie de reglamentos que procuran la cautela de los derechos personales de sus ciudadanos. Recientemente, por ejemplo, ha sido implementada una política de cookies para diversas páginas web.

IBM hizo esfuerzos por desvincularse de su participación en el holocausto, sin embargo, la correspondencia registrada entre sus principales funcionarios de la época confirma el vínculo. Así, 2002 IBM emitió el siguiente comunicado: "*IBM y sus empleados en todo el mundo encuentran abominables las atrocidades cometidas por el*

régimen nazi y condenan categóricamente cualquier acción que ayude a sus actos indescriptibles." (Frank Walker, 2017)

Luego de narrar el origen de la protección de datos personales en Europa, nos es posible confirmar que la necesidad de proteger los datos privados en este continente obedece a la urgencia de prevenir que un determinado gobierno los utilice para planificar y ejecutar políticas que contravengan los derechos humanos.

1.2. Origen de las normas de protección de datos personales en Estados Unidos

Hecho un rastreo pormenorizado es posible afirmar que la primera declaración en relación a la privacidad y vinculado al derecho de protección de la propiedad privada se dio en Inglaterra, por parte del Primer Ministro William Pitt en 1763, quien dijo que el hombre incluso estando en mucha pobreza, puede desafiar en batalla estando dentro de su hogar a todas las fuerzas de la corona. Podrá existir delicadeza en este, su techo estará a punto de derrumbarse, el viento podrá causar frio dentro de su morada, las fuertes tormentas podrán ser muy fuertes, la lluvia empapará absolutamente todo, pero el Rey de Inglaterra se mantendrá afuera; lo cual se resume en el principio básico de *"a man´s house as his castle"*. Con esta declaración se buscaba respetar la premisa de que la casa de una persona es sólo para ésta como lo es el castillo para el rey y nadie podía ingresar a perturbar esa privacidad individual salvo que tuviera autoridad legal. El hogar del individuo establa protegido frente a requisas injustificadas del gobierno. (Nieves Saldaña, 2011, pp. 280–283)

Luego, en 1868, uno de los jueces más influyentes del periodo posterior de la Guerra Civil en Estados Unidos, Thomas M. Cooley, toma el concepto inglés de "*a man´s house as his castle"* para otorgar la calidad de bien jurídico fundamental el derecho de los ciudadanos a no tener inspecciones arbitrarias en sus domicilios por parte del gobierno con el objetivo de garantizar la protección de sus documentos personales, su domicilio y privacidad, ello en base a la Cuarta Enmienda de la Constitución Americana, que prohíbe el registro infundado de las residencias de los ciudadanos.

El primer caso en el que se aplicaron los argumentos de Thomas M. Cooley fue en el caso de *Boyd v. United States* en 1886. En este caso, la Corte Suprema de Estados Unidos consideró que el ingreso a la vivienda de una persona con la finalidad de incautar libros y documentos privados para ser utilizados en juicio penal contra esta persona es equivalente a que esta persona exhiba documentos para auto incriminarse, declarar contra sí mismo y ser testigo en su contra, y por lo tanto esta incautación de documentos contraviene lo establecido en la Cuarta y Quinta Enmiendas de la Constitución americana (*Boyd v. United States*, 1886, p. 116).

Otro caso en el que se aplicaron los argumentos de Cooley fue el de *Olmstead v. United States*, este caso trata sobre las intervenciones secretas de escuchas y registros de conversaciones telefónicas realizada por oficiales del gobierno a sospechosos de violar las normas de importación y venta de bebidas alcohólicas. Las escuchas se realizaron fuera del domicilio de los investigados, sin efectuar ningún allanamiento, por lo que la Corte Suprema determinó que la obtención de estos medios probatorios no contravino la Cuarta Enmienda, pues no implicó el ingreso físico de los oficiales en el domicilio u oficinas de los investigados, ya que las escuchas realizadas en secreto se efectuaron por un cable intervenido por un funcionario del gobierno en el sótano de un edificio o en la vía pública; en consecuencia, al ser las escuchas legales, la exhibición de estos medios probatorios en juicio no implicaba que se interprete que el acusado estuviese declarando en su propia contra. En este caso, el Tribunal hace una aplicación estricta y literal de la Cuarta y Quinta Enmienda indicando que estas están referidas a individuos, inmuebles y documentos y no aplican para prohibir las escuchas o la vista de determinados hechos. (*Olmstead v. United States*, 1928, p. 277)

La posición de la Corte Suprema en el caso de *Olmstead v. United States* trajo consigo una serie de críticas, pues uno de los magistrados del Tribunal Supremo, Lois D. Brandeis, votó en discordia. El magistrado indicaba que sí existía una vulneración de la Cuarta Enmienda, pues los avances tecnológicos invasivos de la privacidad de los individuos, especialmente aquellos que permitían interceptar las comunicaciones por cable eran equivalentes e incluso hacían la interceptar que la de la correspondencia; indicaba, además, que la interceptación telefónica sí vulnera la privacidad de los individuos, precisando que el principio de "*the right to be let alone*" se debe interpretar

de manera amplia, prohibiendo la intromisión del gobierno en la intimidad de las personas sea cual fuere el medio empleado. (Nieves Saldaña, 2011, pp. 284–285)

Pero en realidad, es el avance de la tecnología en fotografía el que provoca el verdadero nacimiento del derecho de privacidad en Estados Unidos. Los fotógrafos tenían que preparar sus propias placas antes de tomar sus fotografías, teniendo que cargar un laboratorio consigo (sustancias y sensibilizadores) para poder revelar sus fotos casi inmediatamente después de haberlas tomado; pero luego de 1890 tomar fotografías se hizo una tarea mucho más fácil; cualquier persona, sin pericia alguna, podía adquirir en el mercado placas listas para su uso, en rollos que podrían, luego, ser revelados. Es así, que para ese entonces las cámaras "Kodak" eran ya livianas y venía cargadas con un rollo de película que permitía tomas hasta 100 fotografías de manera muy sencilla, y no se requería tener mayor destreza técnica para poder tomarlas. (Raydan, 2013, pp. 133–135)

La facilidad que proporcionaba la tecnología en fotografía en 1890 hizo que la prensa sensacionalista americana la provechase para publicar fotos de la vida cotidiana y privada de las personas. A la gente, desde luego, le molestaba que le tomasen fotografías sin su consentimiento, en lugares privados, y que además éstas fueran publicadas en los diarios, por lo que solicitaron en reiteradas oportunidades que se dejase de producir este tipo de contenido; sin embargo, no contaban con una norma que amparase una acción legal para sustentar esta petición y hacer respetar su derecho a la privacidad. Es así como Samuel Warren y Lois Brandeis tomaron el concepto inglés de William Pitt de "*a man´s house as his castle"* para fundamentar el derecho a ser dejado solo ("*right to be let alone*") que, a su vez, se basa en el derecho de privacidad, a disfrutar de la vida y a no ser molestado.

Warren y Brandeis buscaban proteger el derecho a la privacidad individual y evitar que el núcleo de su personalidad y privacidad de los ciudadanos se viera afectado por publicaciones de terceros, sin consentimiento previo. Argumentaron que toda persona tiene el derecho de controlar su propia información y a decidir qué información se publica a terceros y cuál se conserva en su esfera personal y privada, también por protección del ámbito psicológico de la persona. (Nieves Saldaña, 2012, pp. 207–213)

Como venimos exponiendo, el derecho de privacidad en Estados Unidos, a diferencia de otros países, no está expresamente contenido en su Constitución; ha sido la Corte

Suprema la que se ha encargado de hacer respetar este derecho a través de la jurisprudencia, considerándolo como un derecho implícitamente contenido en las garantías de la Primera, Cuarta, Quinta, Novena y Decimocuarta Enmiendas. (Nieves Saldaña, 2011, p. 280)

Es de notar que, a diferencia del caso europeo, el derecho de privacidad en Estados Unidos nace bajo un concepto amplio, desarrollado por la jurisprudencia y fue evolucionando desde la noción de protección de la privacidad en los domicilios hasta llegar a la protección de datos personales, a raíz de una controversia entre particulares que querían evitar la publicación de sus fotos en los diarios de la época, buscando proteger su derecho de privacidad y al honor. Es el caso que, en Estados Unidos es muy poco frecuente que se impongan límites al derecho de información de sus ciudadanos, más aún cuando se trata de información que está referida a funcionarios públicos, ya que estos, se supone, deben tener una conducta ejemplar.

Recordemos el escandaloso *impeachment* efectuado en contra del expresidente de Estados Unidos William Jefferson Clinton en 1998 por mentir bajo juramento y obstruir la justicia respecto de su romance con la entonces pasante y trabajadora de la Casa Blanca Monica S. Lewinsky. Clinton salió librado pues logró obtener los votos necesarios para la absolución de todos los cargos por parte del Senado. El voto mayoritario de la Cámara de Representantes y a favor de que haga público, a través de Internet, el Informe de Kenneth Starr, logrando que en cuestión de minutos, desde cualquier parte del mundo, millones de personas puedan descargar este archivo accediendo a información detallada, explícita y sin censura de la intimidad sexual de Clinton y Lewinsky. En este caso es claro que se priorizó la transparencia, incluso de la vida íntima del presidente del país, por sobre la privacidad entre él y de Lewinsky, quien también tenía un cargo público al trabajar en la Casa Blanca. (STARR, 1998, pp. 4–10)

1.3. Origen de las normas de protección de datos personales y la importancia del derecho de acceso a la información en Latinoamérica

Desde mediados de la década de 1960, y hasta cerca de finales del Siglo XX, Latinoamérica padeció de la imposición de regímenes dictatoriales militares en varios países. En tales regímenes se dieron casos de desaparición forzada, detenciones

arbitrarias, torturas y otros a fin de reprimir a disidentes y para controlar las movilizaciones ciudadanas que se daban producto de las crisis políticas y económicas de la época. Parte importante de la estrategia de estas prácticas militares se dio en mérito a la recopilación y tratamiento de información personal e información política de las personas a ser vigiladas, así como aquellas a las que se quería secuestrar para ejecutarlas posteriormente. (Molina Theissen, 1988, pp. 65–73)

"La generación perdida", como se conoció a la del grueso de víctimas durante la dictadura militar de Jorge Videla en Argentina (1976 - 1983) es un claro ejemplo de esta terrible situación. En efecto, además de los más de 30.000 desaparecidos durante este régimen, se habla también de la "generación perdida" para referirse a los recién nacidos que fueron arrebatados a sus madres gestantes, pertenecientes a la organización guerrillera de la izquierda peronista de los Montoneros. Así, miles de mujeres fueron secuestradas en centros clandestinos y asesinadas luego de dar a luz; los recién nacidos fueron distribuidos entre fascistas y familias afines al gobierno con identidades fraguadas a través de la falsificación de documentos públicos. Con el retorno de la democracia en Argentina, organizaciones como las de "Abuelas de la Plaza de Mayo" ayudan a las familias biológicas de los recién nacidos a encontrarlos. (Cavanagh & Hernández, 2016) Incluso el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto de Argentina tiene activa una campaña internacional por el Derecho a la Identidad que también ayuda a las víctimas de estos delitos a reencontrarse en base a la comparación de pruebas genéticas del Banco Nacional de Datos Genéticos (BNDG). (Ministerio de Relaciones Exteriores, 2017)

En Chile ocurrió algo semejante. A través de la Dirección de Inteligencia Nacional (DINA) de dicho país, bajo el régimen de Augusto Pinochet, se cometieron detenciones ilegales, actos de tortura y asesinato en diversos Centros Clandestinos de Detención, Tortura y Exterminio bajo un sistema de información muy bien organizado, que contaba con información detallada de las personas que eran consideradas "subversivas", cuyos domicilios eran allanados intempestivamente.

Los miembros de la DINA estaban muy bien organizados dentro de estos centros clandestinos de detención: al ingresar un detenido, se le registraba e inclusive se le identificaba con un número para que luego ingresase a otro ambiente de interrogatorio y

tortura. Al inicio de la dictadura chilena surgieron innumerables demandas de *habeas corpus* por casos de detención arbitraria, las que no fueron atendidas; se dieron también varios casos en los que los padres de los detenidos se acercaban a las autoridades a solicitar información respecto del lugar de detención de sus hijos, sin obtener respuesta alguna por parte de las autoridades; en ciertos casos, incluso, éstas negaban que alguien estuviera detenido. Asimismo, ante los allanamientos violentos en los hogares de distintos ciudadanos, los recursos de protección interpuestos eran también desestimados injustificadamente. (Morales Campos, 2018, pp. 14–26)

En nuestro país, por otra parte, casos de corrupción ocurridos, entre los que destaca, a finales de la década de 1990, durante el gobierno de Alberto Fujimori, el de Vladimiro Montesinos, que, teniendo el grado de Jefe del Servicio de Inteligencia Nacional (SIN) y como Consejero de Seguridad del gobierno obtenía ilícitamente dinero del Estado para sobornar a distintos funcionarios públicos, empresarios, representantes de medios de comunicación y otros, a fin de obtener beneficio propio y en favor de terceros instaurando un red de corrupción que impidió el acceso a la información pública de la ciudadanía en general. La manera en la que Montesinos obtenía dinero era solicitando presupuesto y desembolsos al Ministerio de Economía y Finanzas para ser, supuestamente, utilizados en el Ministerio de Defensa, Ministerio del Interior, Fuerza Aérea o Marina de Guerra del Perú para proyectos o compras que tenían la calidad de "reservadas" en actividades de inteligencia y contrainteligencia de carácter secreto (Sentencia Exp. 011-2001, 2001, p. Fundamento. 18).

Montesinos logró obtener hasta 2 mil millones de dólares del estado peruano, estas autorizaciones de presupuestos y desembolsos eran emitidas por los ministerios antes señalados mediante la expedición reservada de decretos legislativos, resoluciones, directamente a través de la firma cheques, etcétera. De esta manera se implantó dentro de las diversas esferas del gobierno una cultura del secreto del gasto y respecto de la rendición de gastos, ya que nadie podía acceder a esta información y, si algún trabajador o funcionario proporcionaba documentos, era destituido y enjuiciado inmediatamente. (Congreso de la República del Perú, 2002, pp. 2556–2558)

En la conocida "Salita del SIN", Montesinos se encargaba de grabar con cámaras y micrófonos ocultos, por supuesto, sin consentimiento, las conversaciones privadas en las

que negociaba y corrompía a funcionarios públicos, entre ellos congresistas, jueces y magistrados integrantes del Tribunal Constitucional de entonces. En las grabaciones quedaban registradas las entregas de dinero en efectivo a estas personas, las que lo recibían a cambio de cumplir con los pedidos de Montesinos. Cuando estos videos (conocidos como "vladivideos") fueron entregados y actuados como medio probatorio en juicios que se iniciaron al terminar el régimen de Fujimori, los acusados argumentaron que estos videos no podían ser considerados como medios probatorios lícitos, pues las grabaciones se habían efectuado sin su consentimiento y, por lo tanto, vulneraban su derecho a la intimidad. Al respecto, los juzgados a cargo consideraron que estos videos sí eran válidos y serían tomados en cuenta a efectos de acreditar los delitos, pues luego de efectuar una ponderación entre del derecho a la privacidad y el derecho de transparencia, prima la transparencia y la búsqueda de la verdad. (*Sentencia Exp. 21-2001*, 2003, p. Fundamentos 2, 3 y 8)

A raíz de los hechos narrados anteriormente, una vez llegados a su fin los regímenes dictatoriales en América Latina, era evidente la necesidad de reconstruir la democracia, y para ello era indispensable conocer la verdad sobre todas las personas desaparecidas, no solo para sancionar a los culpables, sino también para que, asumida la responsabilidad de lo ocurrido, los gobiernos pudieran empezar una nueva era basada en el principio de transparencia. Consecuencia de ello, la necesidad de crear una base legal que garantice a los ciudadanos acceder a información pública.

1.4 Breve análisis de las diferencias entre las vertientes europeas, americanas y latinoamericanas de derecho de resguardar los datos personales y dar paso de poder entrar a la información (transparencia)

Podemos decir que las diferencias entre las restricciones que se dan en Estados Unidos y Perú son muy marcadas. En Estados Unidos el derecho a la privacidad está más enfocado al consumidor, al punto que no tiene reconocimiento constitucional, sino más bien uno de carácter jurisprudencial, las empresas no necesitan el control previo de recopilación de datos y tienen permitido recabar todo tipo la información de sus clientes (mientras estos manifiesten su conformidad), incluso si no está vinculada directamente al servicio contratado o al trato acordado. Por su parte, en Perú el derecho de protección de datos personales está protegido con rango constitucional y las empresas sólo pueden

recabar datos que están vinculados a la obediencia de los deberes tomados por la empresa y el usuario para los fines especificados en el contrato.

En base a lo expuesto en este capítulo, vemos que, mientras en Europa era importante que los gobiernos regularan la protección de datos personales, su tratamiento y flujo transfronterizo debido a la vulneración de estos derechos ocurrida en el Holocausto, en Latinoamérica, una vez culminados los regímenes militares de segunda mitad del Siglo XX, se consideró necesaria una mayor protección al derecho que se tiene a poder ingresar a la información que el Estado puede otorgarnos al ser de carácter público, una aplicación de políticas de transparencia claras, así como brindar a los ciudadanos acceso a mecanismos eficientes que les permitieran, a su vez, dar con información pública.

Es en ese sentido, teniendo en cuenta los antecedentes históricos de los países latinoamericanos, que vemos que lo que realmente debe primar es el derecho al acceso a la información pública por encima del derecho de protección de datos personales. No deja de sorprender que, a pesar de lo acontecido en los regímenes militares y la gran corrupción, en el Perú, la norma peruana de protección de datos personales, Ley N° 29733, del 3 de julio de 2011, sea un fiel reflejo de la norma europea, debido a que colisiona en ciertos aspectos con lo dispuesto por la Ley de Transparencia y Acceso a la Información Pública, Ley Nro. 27806, publicada el 13 de julio de 2002. Por ello, consideramos que países como Perú deberían enfocarse en fortalecer la transparencia y sancionar severamente a las entidades estatales que no cumplan con ofrecer el servicio de tomar atención en cuanto a las solicitudes para poder ingresar a toda la información de sus ciudadanos.

CAPÍTULO II

DERECHO DE PROTECCIÓN DE DATOS PERSONALES

2.1. Definición de derecho de protección de datos personales

Se justifica la existencia de la protección de datos personales para garantizar a la persona el control autónomo e independiente de su propia individualidad, privacidad e información, de cualquier dato que le pertenezca, la identifique o la haga identificable; asimismo, en caso la persona proporcione cierta información de su pertenencia, a favor de un tercero, sea éste el Estado o una entidad privada, tiene derecho a saber que uso se le va a dar a su información, el destino y tráfico de la misma. Así, está prohibido que esta información tenga una finalidad ilícita o afecte otros derechos fundamentales de la persona. Además de dar la garantía antes expuesta, este derecho faculta al afectado a interponer recursos de oposición a los datos personales que sean utilizados con una finalidad distinta a la que justificó su obtención.

En Perú, este derecho se caracteriza por tener un reconocimiento constitucional y por proporcionar una serie principios reglas y mecanismos que tienen como objetivo proteger la recopilación y el tratamiento de los datos personales que los ciudadanos proporcionan a diversas entidades, públicas o privadas, y así poder acceder a diferentes bienes y servicios o incluso ejercer otro tipo de derechos. La protección de este derecho se originó en la Constitución de 1993, siendo que el inciso 6, del artículo 2 se señala lo siguiente:

> *" Artículo 2°.- Toda persona tiene derecho: (...) 6.- A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.*

Pero no es hasta el año 2011, ante la exigencia para la suscripción de aquellos Tratados de Libre Comercio (TLC) dándose entre diversos países, que el Estado Peruano se vio en la obligación de promulgar la Ley Nro. 29733, Ley de protección de datos personales (LPDP), publicada el 03 de julio de 2011, así como su Reglamento, contenido en el Decreto Supremo N° 003-2013-JUS, publicado el 22 de marzo de 2013 (Reglamento de la LPDP). Estas dos normas fueron modificadas significativamente en 2017, a través del Decreto Legislativo N° 1353, que crea a la Autoridad Nacional de Transparencia y

Acceso a la Información Pública y fortalece el Régimen de Protección de datos Personales y la regulación de la gestión de intereses.

Estas normas basan el amparo de datos personales sobre el derecho a la autodeterminación informativa, pues como ya lo hemos dicho anteriormente, su objetivo es proteger la privacidad de las personas o la privacidad que se debe tener en familia, se deben de proteger también como es la reputación o secreto frente a los constantes peligros que representa el poder usar o incluso cambiar información de aquellos datos a través de los aparatos electrónicos que benefician dichos cambios. (Sentencia TC Exp. No 01797-2002-HD/TC, 2003, Fundamento 2-4)

2.2. Sujetos y autoridades vinculadas a la aplicación de la legislación de protección de datos personales

La LPDP identifica a diversos sujetos a los que les afecta la aplicación de la norma en diferentes niveles. En primer término, apunta a los ciudadanos titulares de los datos que serán materia de recopilación y tratamiento; en segundo término, a la entidad que es titular del banco de datos y que es responsable del tratamiento; y, en tercer término, desde el lado institucional, está la Autoridad Nacional de Protección de Datos Personas (ANPD).

El titular de los datos personales es aquella persona mayor de edad que da su consentimiento para que un tercero pueda recopilar y tratar sus datos para una finalidad determinada. Los niños y adolescentes tienen que ejercer este derecho a través de sus representantes legales; es de advertir, al respecto, que los titulares de bancos de datos deben garantizar que los datos pertenecientes a los niños y adolescentes sean empleados con especial cuidado.

El titular del Banco de Datos personales puede ser alguna entidad estatal o una privada que guarda, organiza y permite el acceso a una serie de datos personales, en diferentes soportes físicos, digitales, magnéticos u otros.

Por otro lado, el Responsable del Tratamiento de Datos Personales es aquella entidad estatal o privada, que bien puede ser el Titular del Banco de Datos o un tercero, siempre

que en mérito a una relación contractual con este último efectúa el tratamiento de datos personales mediante procedimientos técnicos, automatizados o no, que permite la recopilación, registro, organización, almacenamiento, modificación, utilización, supresión y difusión de data.

Por último, la Autoridad Nacional de Protección de Datos Personas (ANPD), es la autoridad administrativa que empezó a funcionar desde el 2017 y que está adscrita al Ministerio de Justicia y Derechos Humanos, y que tiene como funciones la de normar, supervisar, fiscalizar, orientar, dar opinión técnica, resolver reclamaciones, iniciar acciones de fiscalización de oficio o por denuncia del agraviado con capacidad sancionadora y coactiva, entre otros. Asimismo, la ANPD está encarga del Registro Nacional de Protección de Datos Personales en el que se inscriben: los bancos de datos personales tanto de la administración pública como los de las entidades privadas a nivel nacional, las comunicaciones de flujo transfronterizo de datos personales y las sanciones, medidas correctivas o medidas cautelares impuestas por la ANPD entre otros.

En 2021, la ANPD impuso multas por la suma de S/ 6´084,113, de las cuales se recaudó un total S/1´868,135.89. La diferencia se debió, en buena medida, a que algunas de las entidades sancionadas se acogieron al beneficio de descuento del 40% por pronto pago. (Autoridad Nacional de Protección de Datos Personales, 2022, p. 13)

2.3. Ejercicio del derecho de protección de datos personales

Quien de a conocer que su derecho a la protección de datos personales ha sido afectado, puede solicitar directamente al titular de la base de datos o al responsable de su tratamiento, acceso a su información personal. Para ello, puede optar por un procedimiento de tutela directa, suprimir y oponerse al tratamiento de sus datos cuando no haya prestado el consentimiento previo o no haya sido debidamente informado de la finalidad para la cual se recopilaron sus datos. El destinatario de una solicitud de este tipo tiene 8, 10 o 20 días para responder a la petición respectiva. El plazo específico dependerá de si la solicitud está referida al ejercicio de información, acceso a la información o rectificación, cancelación u oposición. En caso el titular de la base de datos o el responsable de su tratamiento justifique la necesidad de que el supuesto afectado presente

más documentación, se lo deberá de comunicar dentro de los 7 días siguientes desde que recibió su solicitud, otorgándole 10 días para presentar estos agregados.

En caso el titular de la base de datos o el responsable de su tratamiento deniegue el pedido del afectado, la respuesta que éste reciba no sea satisfactoria o simplemente ésta no se dé, el afectado puede acudir ante la ANPD e iniciar un procedimiento trilateral de tutela. En él, dicha autoridad resolverá el requerimiento del afectado en el plazo de 30 días, los que se pueden ampliar por 30 días más. El órgano resolutor en este caso es la Dirección General de Protección de Datos Personales. Cabe señalar que contra sus resoluciones procede recurso de reconsideración, que, de ser resuelto, agota la vía administrativa. Tratándose de un procedimiento administrativo, se rige conforme a la Ley del Procedimiento Administrativo General (Ley Nro. 27444). En este contexto, la ANPD puede emitir medidas cautelares y correctivas de carácter provisional.

Independientemente de lo antes indicado, es posible acudir al Poder Judicial a través de una Acción de Habeas Data, conforme a lo dispuesto por el Código Procesal Constitucional.

Sea cual fuera el procedimiento mediante el cual el supuesto afectado ejerza su derecho de protección de datos personales, también puede reclamar en la vía civil la indemnización correspondiente por los daños y perjuicios que le fueran ocasionados.

2.4. Inteligencia artificial y gestión de datos personales, medidas de seguridad en el caso Cambridge Analytica

La Comisión Federal de Comercio de Estados Unidos de América (Federal Trade Commission - FTC) demandó a la empresa Cambridge Analytica LLC, así como a dos de sus funcionarios Aleksandr Kogan (KOGAN) y Alexander James Ashburner Nix (NIX) por cometer actos y prácticas engañosas para recopilar información personal de los usuarios de Facebook y tratarlos con fines publicitarios políticos y comerciales.

Cambridge Analytica LLC es una sucursal de la empresa británica S.C.L Group y

opera como una empresa de consultoría y análisis de datos que brinda servicios de marketing y perfiles de votantes. S.C.L Group creó a Cambridge Analytica LLC como su sucursal en Estados Unidos para atender a sus clientes que participaban en las elecciones estadounidenses del proceso de 2016.

En paralelo, tenemos a Facebook Inc., empresa que, en su aplicación electrónica utiliza una interfaz de programación de aplicaciones denominada "GraphAPI" que puso a disposición de los terceros desarrolladores de su plataforma. A través de GraphAPI, Facebook podía a acceder a datos personales de sus usuarios y de los amigos de estos, guardando registro de los “me gusta” dados a páginas públicas de Facebook, así como la siguiente información de cada usuario conectado a sus aplicaciones:

- Cumpleaños
- Biografía
- Actividades
- Actividad de artículos periodísticos
- Actividad de libros
- Registros
- Ciudad actual
- Historia de la educación
- Eventos
- Actividad física
- Actividad de juegos
- Grupos
- Ciudad natal
- Intereses
- Gustos
- Actividad musical
- Notas
- Presencia en línea
- Actividad de Open Graph
- Fotos
- Preguntas
- Relaciones
- Detalles de la relación
- Religión/Puntos de vista políticos
- Estado
- Suscripciones
- Vídeos
- Actividad de visualización de videos
- Url del Sitio Web
- Historial de trabajo

El modelo central de negocio de Facebook se basa en el uso de la información que recopila de sus usuarios para publicidad y venderla a terceros desarrolladores de otras aplicaciones que funcionan a través de Facebook. El problema con Facebook era que durante mucho tiempo estuvo vendiendo la información privada de sus usuarios y de los amigos de estos usuarios (incluso sin que estos amigos tengan interacción directa con las aplicaciones de Facebook) sin que estos hayan prestado su consentimiento o hayan tenido conocimiento de lo que se hacía con su información, motivo por el cual Comisión Federal de Comercio ya había sancionado anteriormente a la compañía.

Una de las personas que tenía una aplicación con acceso a información de Facebook con la versión GraphAPI era KOGAN, con una aplicación denominada CPW LAB,

motivo principal por el que Cambridge Analytica buscó trabajar con él y tener a su disposición esta aplicación.

El objetivo de Cambridge Analytica, KOGAN y NIX era obtener información de los usuarios de Facebook a través de la aplicación CPW LAB, para alimentar con ella un algoritmo a través del cual predecir la personalidad de un individuo en función a los "me gusta" que se cliquean en las páginas públicas de Facebook. NIX y KOGAN afirmaban que, por ejemplo, dar "me gusta" a páginas de Facebook relacionadas con: ¿Cómo perder a un chico en 10 días?, George W. Bush, rap e hip-hop podría vincularse con una personalidad conservadora y convencional. Afirman, además, que su algoritmo era tan preciso que podía predecir la personalidad de una persona mejor que los compañeros de trabajo, los amigos, la familia e incluso su propia esposa(o). Con la información resultante del procesamiento de datos con este algoritmo, Cambridge Analytica, KOGAN y NIX podían ofrecer perfiles de votantes, microtargeting y otros servicios de marketing para campañas de EE. UU. y otros clientes con sede en EE. UU.

En este punto, es importante hacer mención que Facebook había anunciado en abril de 2014 que estaba introduciendo una nueva versión de GraphAPI (v.2), que ya no permitiría a los desarrolladores recopilar datos de perfil de amigos afectados, solo de los propios usuarios de la aplicación y de las aplicaciones existentes que fueron ingresadas con un año de anterioridad a la entrada en vigencia de las nuevas limitaciones; de hecho, las aplicaciones que tenían menos de un año serían limitadas automáticamente. En el caso en concreto, la aplicación de KOGAN tenía más de un año en Facebook y por lo tanto fue "exenta" de las nuevas limitaciones de acceso a la información de GraphAPI (v.2) en la recopilación de datos, por lo que pudo utilizar varias herramientas que le proporcionaba GraphAPI (v.1); esto mismo convirtió a KOGAN en un socio atractivo para Cambridge Analytica.

Cambridge Analytica, KOGAN y NIX, crearon la "Aplicación GRS", conocida en Facebook mismo como "*This is your digital life*", ello porque con esta aplicación y con una escala "Océano" recopilaban datos de los usuarios de Facebook y de los amigos de éstos dirigiendo encuestas a los usuarios ubicados en Estados Unidos. Estas encuestas tenían preguntas referidas a temas de interés de los clientes de Cambridge Analytica, como, por ejemplo, respecto de preferencias en el ámbito político, la frecuencia en la

votación, el grado de consistencia en votos emitidos en favor de un mismo partido político, y otros respecto de variedad de temas controvertidos particulares. A los usuarios que completaban estas encuentras y autorizaban la recopilación de la información de su perfil de Facebook se les pagaba pocos dólares por hacerlo; sin embargo, no se les informaba que la "Aplicación GRS" también podía acceder y recopilar la información de sus amigos.

Según la Comisión Federal de Comercio, GraphAPI recopiló datos de perfil de usuario de Facebook de aproximadamente 250,000 a 270,000 usuarios de Facebook que interactuaron directamente con la aplicación, así como de 50 a 65 millones de "Amigos", es decir, de no usuarios directos. Con la obtención de toda esta información, los algoritmos empleados por KOGAN y NIX proporcionaron puntajes de personalidad para los Usuarios que llenaron las encuestas y para los "Amigos" de estos; los resultados fueron tan buenos que podían compararse con los del registro regular de votantes de los Estados Unidos.

Es recién a finales del año 2015 que se empezaron a hacer públicos informes referidos al uso de datos que Facebook había proporcionado a Cambridge Analytica, y es en mérito a ellos que Facebook ordena a KOGAN, NIX y Cambridge Analytica eliminar todos los datos que tuvieran hasta el momento en su poder y/o que hubiesen sido obtenidos a través de Facebook. Si bien estas entidades cumplieron con eliminar los datos, las personas o entidades clientes de Cambridge Analytica aún tenían en su poder estos datos y los modelos de datos basados en ellos, obtenidos de los usuarios de Facebook.

Cuando la Comisión Federal de Comercio inicia sus investigaciones en contra de Facebook, Cambridge Analytica, KOGAN y NIX; Cambridge Analytica se declaró en quiebra. KOGAN y NIX llegaron a un acuerdo con la Comisión, por el que se restringe la forma en que podrán operar a futuro con otras empresas. Por su parte, Facebook recibió una multa de $ 5 mil millones de dólares, además de tener que adoptar una serie de restricciones para evitar nuevos posibles problemas en términos de privacidad datos de sus usuarios en el futuro. Asimismo, Facebook debió reestructurar su Junta Corporativa para incluir mecanismos sólidos de protección de datos de los usuarios, así como gestionar la realización periódica de auditorías llevadas a cabo por terceros y verificadas por la Comisión Federal de Comercio.

El monto de la multa impuesta en contra de Facebook fue fijada en consideración a que la compañía no había respetado las medidas de seguridad impuestas en 2012. Se trata de la multa más cuantiosa jamás impuesta a una empresa por violación de la privacidad de los consumidores. Equivale a casi veinte veces el valor de la sanción más grande por privacidad o seguridad de datos jamás impuesta en todo el mundo, y es, actualmente, la multa más grande jamás impuesta por el gobierno de los EE.UU por cualquier clase de violación.

Como queda claro de este caso, la sanción apunta sobre todo a la mala fe y al engaño, tanto por parte de Facebook, que incumplió de manera reiterada las políticas de privacidad de los datos de sus usuarios, y de KOGAN, NIX y Cambridge Analytica, que engañaron a sus usuarios señalando que sólo accederían a sus datos, siendo que en realidad accedieron a la de sus amigos. Es claro que los usuarios no habían dado su consentimiento para ello y no tenían conocimiento de la finalidad del uso de sus datos por parte de la "Aplicación GRS", ni de la aplicación de algoritmos especiales como aquellos con los que contaban. Es claro, también, que la sanción impuesta por la Comisión Federal de Comercio sanciona además la falta de transparencia, en general, por parte de todos los involucrados.

A lo antes dicho, debemos agregar que hay quienes afirman que la "Aplicación GSR" de Cambridge Analytica tuvo un papel clave en las votaciones de las elecciones presidenciales de Estados Unidos, ya que, al contar con perfiles psicológicos de cada usuario, el diseño de la publicidad personalizada con contenido específico para influir en las decisiones políticas de una persona en relación a tal o cual candidato, era evidente, podía ser mejor realizado. A propósito, Cambridge Analytica incluso emitía y replicaba por redes sociales noticias falsas "fake news". (BBC Mundo, 2018)

CAPÍTULO III

DERECHO AL ACCESO A LA INFORMACIÓN

3.1. Contexto en el que se crea y aplica la Ley de Transparencia y Acceso a la Información Pública y la creación de la Autoridad Nacional de Transparencia y Acceso a la Información Pública en el Perú

Según Transparencia Internacional, Perú tiene una calificación de 36/100 en el ranking global en el Índice de Percepción de la Corrupción (IPC) del sector público, posicionándose en el puesto 105 de 180. (Transparencia International, 2021)

Por otro lado, de las encuestas sobre percepción de corrupción efectuada por Proética nos señala que el 61% de los encuestados considera que la corrupción y las coimas están dentro de los tres problemas más graves que tiene el país luego de la delincuencia y falta de seguridad. (Proética, 2021)

En el debate que sostuvieron los congresistas integrantes de la Comisión de Constitución para la aprobación de la Ley de Transparencia y Acceso a la Información Pública, hubo que señalar que, según lo indicado por Defensoría del Pueblo y el Ministerio de Economía y Finanzas, para el año 2001, la carencia de transparencia en las entidades públicas del país se evidenciaba de la siguiente manera:

- El 69,3% de los ministerios y organismos autónomos no publicaban sus proyectos de inversión, y el 57,7% no publica sus presupuestos ejecutados;
- El 90,5% de las empresas públicas no publicaban su presupuesto anual o sus presupuestos ejecutados y el 66,7% no publicaban sus contrataciones y adquisiciones; y
- El 84,4% de las unidades ejecutoras no publicaban su presupuesto anual y su presupuesto ejecutado, y el 92,7% no publicaban sus proyectos de inversión.

Luego de que el gobierno de transición de Valentín Paniagua emitiese el Decreto Supremo Nro. 018-2001-PCM, de fecha 26 de febrero de 2001, mediante el cual se exigió a las entidades públicas que, en un plazo máximo de 30 días hábiles, incorporasen dentro de su Texto Único de Procedimientos Administrativos (TUPA) un procedimiento que posibilite el acceso de las personas a la información que posean o produzcan, se verificó lo siguiente:

- De 234 instituciones del Estado, sólo 66 cumplieron con elaborar un conjunto de procedimientos administrativos para que los ciudadanos tengan acceso a la información, de acuerdo con el Decreto Supremo mencionado; es decir, que más del 70% no cumplieron con lo exigido en la norma en favor del ciudadano.
- Sólo el 27% ya cuenta con un procedimiento sencillo para atender los pedidos. (Congreso de la República del Perú, 2002, p. 2559)

Como se puede apreciar fácilmente de estos datos, Perú padece de un grave problema de corrupción. El uso indebido del poder por parte de un funcionario público para obtener beneficios particulares trae consigo graves consecuencias: entre otros, problemas de carácter económico, al incrementar el costo de los negocios, además de que la desviación de fondos originalmente destinados a prestar servicios básicos como salud, educación, vivienda y otros, acarrea de por sí males tremendos. Además, el impacto negativo en la credibilidad, la percepción negativa que desarrollan los ciudadanos e inversionistas internacionales respecto del gobierno y sus funcionarios implica, lógicamente, nuevas dificultades en toda gestión.

Recién en 2002 se promulga en Perú la Ley Nro. 27806 - Ley de transparencia y acceso a la información pública - (LTAIP). Esta ley aparece luego de que el país atravesara la gran crisis de corrupción que dejó el último gobierno de Alberto Fujimori. A la LTAIP se le suman su Texto único Ordenado, creado mediante Decreto Supremo Nro. 043-2003-PCM y su Reglamento, el Decreto Supremo Nro. 072-2003-PCM. La creación de todas estas normas atiende a lo indicado en el Informe sobre "El Acceso a la Información Pública y la Cultura del Secreto" elaborado por la Defensoría del Pueblo en el 2001, el mismo que señala que en Perú existe una "cultura del secreto", cultura que está sustentada en la negativa reiterada de los funcionarios y autoridades públicas a

proporcionar la información solicitada por los ciudadanos. Esta llamada "cultura de secreto" facilita que los funcionarios públicos ejerzan poder de manera oculta, sin controles, lo que evidentemente genera un ambiente especialmente propicio para el incremento de la corrupción. (Defensoría del Pueblo, 2001, p. 144)

Debemos agregar que quince años después de la promulgación de la LTAIP, el 07 de enero de 2017, se publica el Decreto Legislativo Nro. 1353, con la finalidad de crear la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP) y, por medio de ella, fortalecer el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses.

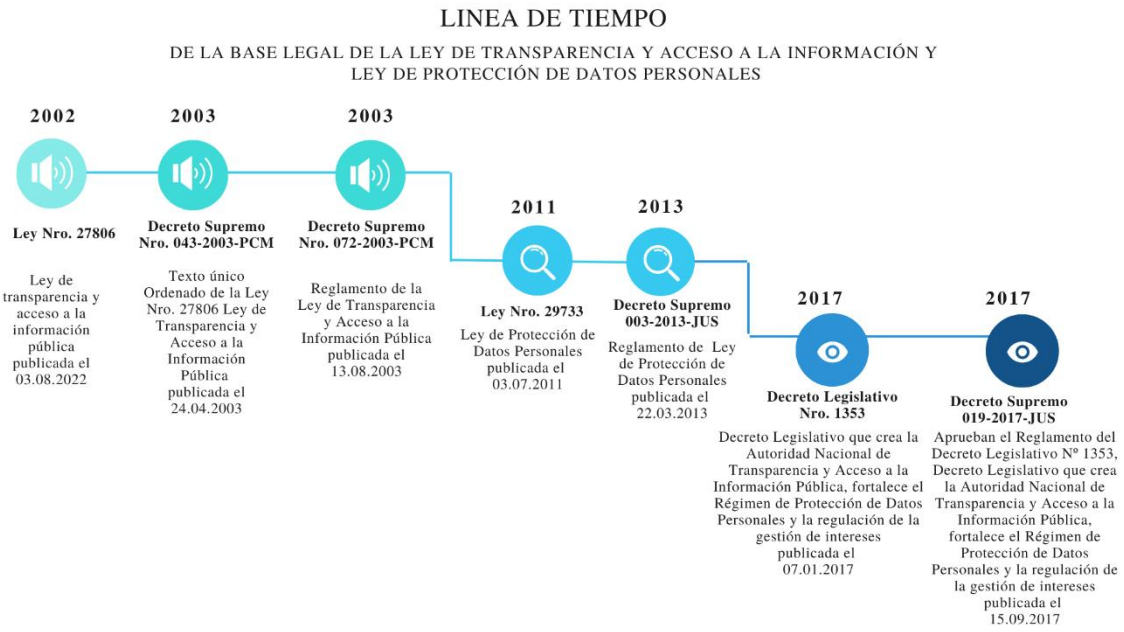

Figura 3

Línea de tiempo de la base legal de la Ley de Transparencia y Acceso a la Información y Ley de Protección de Datos Personales.

Como consta en la línea de tiempo (véase el cuadro anterior), la Ley de Transparencia peruana aparece en 2002, tras el final del régimen de Alberto Fujimori, para que, luego de quince años, recién en 2017, se cree la Autoridad Nacional de Transparencia y Acceso a la Información Pública. Entretanto, fue promulgada la Ley de Protección de Datos Personales.

3.2. Definición de derecho de acceso a la información

Al igual que el derecho de protección de datos personales, el de acceso a la información pública tiene también reconocimiento constitucional en el inciso 5 del artículo 2 de la Carta Magna del Perú. Este derecho se puede definir como aquel que tiene toda persona para acceder, sin tener que exponer mayor motivación, a información a cualquier entidad del Estado, y es que éste tiene el deber de brindarla dentro de los plazos legales y previo pago de los costos que suponga el requerimiento.

Ahora bien, existen limitaciones respecto a la información que puede ser efectivamente requerida. Cuando ésta afecta la intimidad personal y/o cuando la publicación de determinada información esté expresamente prohibida por ley o por razones de seguridad nacional, no será posible.

Es importante señalar que las limitaciones al derecho de acceso a la información únicamente pueden darse por las causales específicamente establecidas en los artículos 15, 15-A y 15-B, de la LTAIP. Estas limitaciones están referidas a información secreta por tratarse de información clasificada del ámbito militar, información reservada por razones de seguridad nacional, información confidencial referida a información deliberativa previa a la toma de una decisión de estado, información referida al secreto bancario, tributario, comercial, industrial, tecnológico y bursátil, información de investigaciones en trámite en procesos sancionadores, información preparada u obtenida por asesores jurídicos o abogados de las entidades públicas cuya publicidad pueda revelar las estrategias legales de defensa e información referida a los datos personales que invadan la intimidad personal y familiar de una persona e información referida a la salud personal.

Las limitaciones al acceso a la información únicamente están referidas a información secreta, reservada y confidencial. Se debe hacer una interpretación restrictiva al momento de clasificar determinada información como secreta o confidencial, pues al limitar el acceso a la información a un ciudadano se le restringe un derecho de carácter fundamental.

Las únicas entidades que pueden acceder a todo tipo de información, sin restricciones, son el Congreso de la República, el Poder Judicial, la Contraloría General de la República y la Defensoría del Pueblo, según lo establecido en el artículo 15-C de la LTAIP. Al respecto, cabe señalar que según lo establecido en el artículo 5 del Decreto Legislativo Nro. 1353 (que crea a la Autoridad Nacional de Transparencia y Acceso a la Información Pública) se establece que todas las entidades públicas que tengan que limitar el acceso al ciudadano de determinada información por ser secreta, reservada y/o confidencial deben elaborar lineamientos para la clasificación y desclasificación de esta información. Los lineamientos que se elaboren por la entidad deben ser aprobados por Decreto Supremo con los respectivos votos aprobatorios por parte del Consejo de Ministros, ser refrendados por el Presidente del Consejo de Ministros, Ministro de Justicia y Derechos Humanos y el Ministro de Economía y Finanzas.

3.3. Sujetos y autoridades vinculadas a la aplicación de la legislación de derecho de acceso a la información

En cuanto a la LTAIP, su TUPA y reglamento nos permiten identificar a los siguientes sujetos a los que se les aplica la norma en diferentes niveles.

Así es que, en primer lugar, evidentemente, están los ciudadanos que solicitan a la entidad pública que les proporcione determinada información.

En segundo lugar, tenemos a las entidades de la Administración Pública, es decir al Poder Ejecutivo (incluyendo Ministerios y Organismos Públicos), Poder Legislativo, Poder Judicial, Gobiernos Regionales, Gobiernos Locales, y los demás organismos estatales a los que Constitución y las leyes confieren autonomía.

En tercer lugar, tenemos a las personas jurídicas que bajo el régimen del derecho privado prestan servicios públicos o ejercen función administrativa.

En cuarto lugar, tenemos al funcionario responsable de entregar la información que designa cada entidad pública. Esta es la persona que tiene como obligación recibir y dar atención a las solicitudes de acceso a la información que lleguen a la entidad dentro de los plazos establecidos por ley, por lo que además es responsable de requerir la

información al funcionario o servidor que posee la información solicitada para luego entregarla al solicitante.

En quinto lugar, tenemos el funcionario o servidor que posee la información; es decir, quien ha creado, obtenido o está en posesión de la información requerida y que se encuentra en la obligación de proporcionarla al funcionario responsable de entregar la información.

Al respecto es necesario precisar que el funcionario que incumple de manera arbitraria con su obligación y obstruye el acceso a la información solicitada, o la proporcione incompleta incurre en falta administrativa, por lo que se le aplica el procedimiento que corresponda según el tipo de contrato que tiene con la entidad; incluso se le puede denunciar penalmente por la comisión del delito de Abuso de Autoridad (Artículo 377 del Código Penal).

En sexto lugar, tenemos a la Autoridad Nacional de Transparencia y Acceso a la Información Pública (La Autoridad). Esta Autoridad, al igual que la Autoridad Nacional de Protección de Datos Personales, está adscrita al Ministerio de Justicia y Derechos Humanos, conforme se aprecia en el siguiente cuadro:

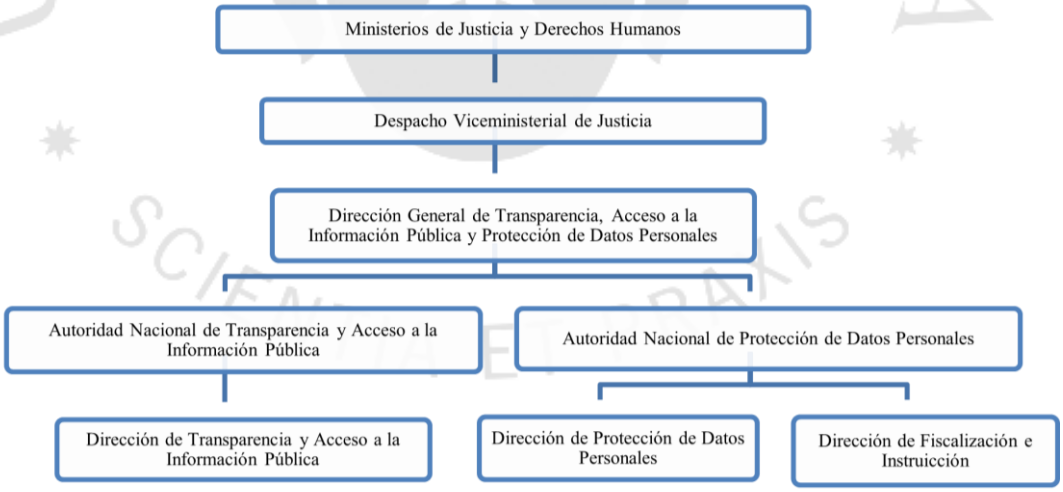

Figura 4

Organigrama del Ministerio de Justicia y Derechos Humanos en el que se verifica la ubicación de la Autoridad Nacional de Transparencia y Acceso a la Información Pública y la Autoridad Nacional de Protección de Datos Personales.

La Autoridad tiene como principal función la de supervisar el cumplimiento de las normas en materia de transparencia y acceso a la información pública, absolver las consultas que personas particulares y otras entidades le formulen, y supervisar el cumplimiento de la actualización de los portales de transparencia.

En sétimo lugar, tenemos al Tribunal de Transparencia y Acceso a la Información Pública (El Tribunal), que es un órgano resolutivo del Ministerio de Justicia y Derechos Humanos. Éste tiene autonomía en el ejercicio de sus funciones y es la última instancia administrativa en materia de transparencia y derecho al acceso de información pública a nivel nacional. Entre las principales funciones que tiene cuenta resolver en última instancia y agotando la vía administrativa las decisiones emitidas por las entidades públicas, resolver los recursos de apelación que interpongan lo funcionarios o servidores públicos que fueron sancionados por falta grave al incumplir las normas de transparencia y acceso a la información pública, así como dirimir a través de opinión técnica vinculante los casos en los que se presente conflicto entre la aplicación de la LPDP y la LTAIP.

Respecto a las Resoluciones del Tribunal que se pronuncian sobre los recursos de apelación que interpongan los funcionarios o servidores públicos que fueron sancionados por falta grave al incumplir las normas de transparencia y acceso a la información pública, tenemos que, desde 2017 a agosto de 2022, el Tribunal ha resuelto 32 apelaciones, de las cuales 8 fueron declaradas improcedentes, 11 resoluciones de emitidas por la entidad fueron declaradas nulas, y 13 apelaciones, fundadas a favor del funcionario público.

Las resoluciones en que se ha declarado improcedente la apelación se justifican en el hecho que quien apela es el denunciante, que al verificar que la entidad ha declarado infundados los hechos denunciados, presenta su recurso de apelación ante el Tribunal. Dicho órgano considera que el denunciante no es parte del procedimiento administrativo disciplinario y, por lo tanto, carece de legitimidad para presentar el recurso de apelación. Bajo esta lógica, el denunciante no posee derecho ni interés legítimo en la imposición del castigo que le permita obtener una satisfacción jurídicamente relevante. Al respecto, consideramos necesario cambiar tal criterio del Tribunal, ya que debería de revisar las resoluciones que absuelvan a los funcionarios en caso hayan cometido falta grave al incumplir lo establecido en la LTAIP. En todo caso, estas resoluciones absolutorias deberían ser confirmadas por el Tribunal de oficio, ello en vista que tratan la comisión de

faltas graves con afectación de un derecho fundamental: el de acceso a la información pública.

Por otro lado, las declaraciones de nulidad de la Resolución de la entidad, así como aquéllas que declaran fundado el recurso de apelación del funcionario público, se amparan en que el procedimiento administrativo sancionador disciplinario ha comprendido actos que no se ajustan al debido proceso. Un ejemplo podría ser el de falta de notificación adecuada a un funcionario, o la tipificación equivocada de una conducta sancionable administrativamente, expresamente establecida en una norma con rango de ley; asimismo, que la entidad no haya cumplido con recabar información relevante para verificar si es que el funcionario ha cometido o no falta grave, o que no se ha motivado correctamente una decisión administrativa.

Como queda claro, estos pronunciamientos del Tribunal no se basan sobre el fondo de la conducta infractora del funcionario público, sino más bien en deficiencias de forma ocurridas en las entidades públicas. Ello demuestra que, en la actualidad, estas entidades aún no están correctamente organizadas, ni su personal debidamente capacitado para llevar adelante este tipo de procedimientos conforme a derecho. Esta situación requiere una intervención decidida por parte del Estado dada la gravedad de la falta que se investiga en cada caso, puesto que implica una posible lesión al derecho constitucional de acceso a la información.

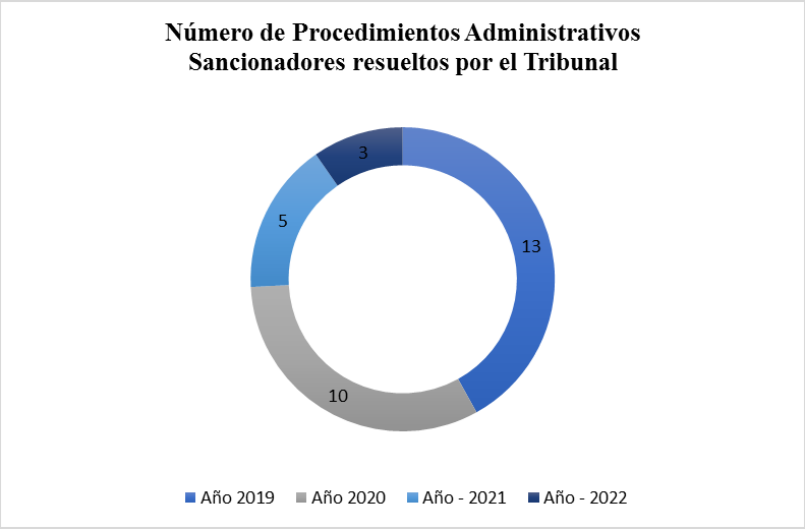

Figura 5
Gráfico en el que se muestra el Número de Procedimientos Administrativos Sancionadores resueltos por el Tribunal de Transparencia y Acceso a la

Información Pública. Se precisa que en 2017 y 2018 el Tribunal no recibió recursos de apelación por infracciones a las normas de transparencia y acceso a la información pública.

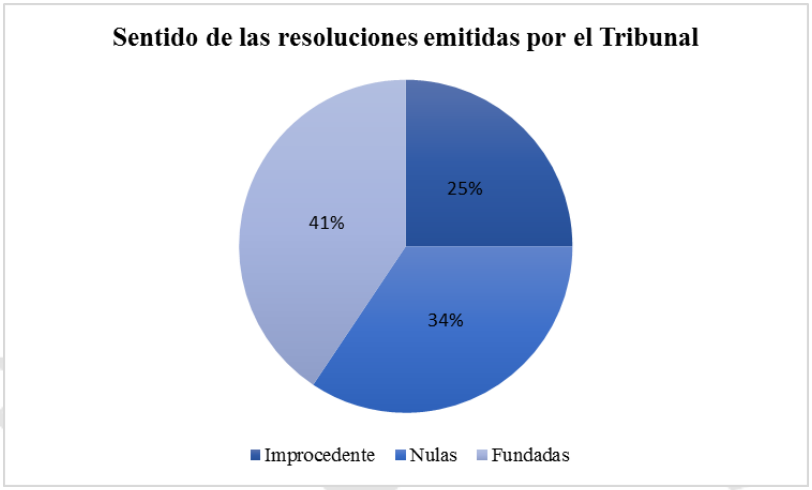

Figura 6

Gráfico en el que se verifica el sentido de las resoluciones del Tribunal de Transparencia y Acceso a la Información Pública, la mayoría de las cuales han declarado fundados los recursos de apelación presentados por los funcionarios públicos.

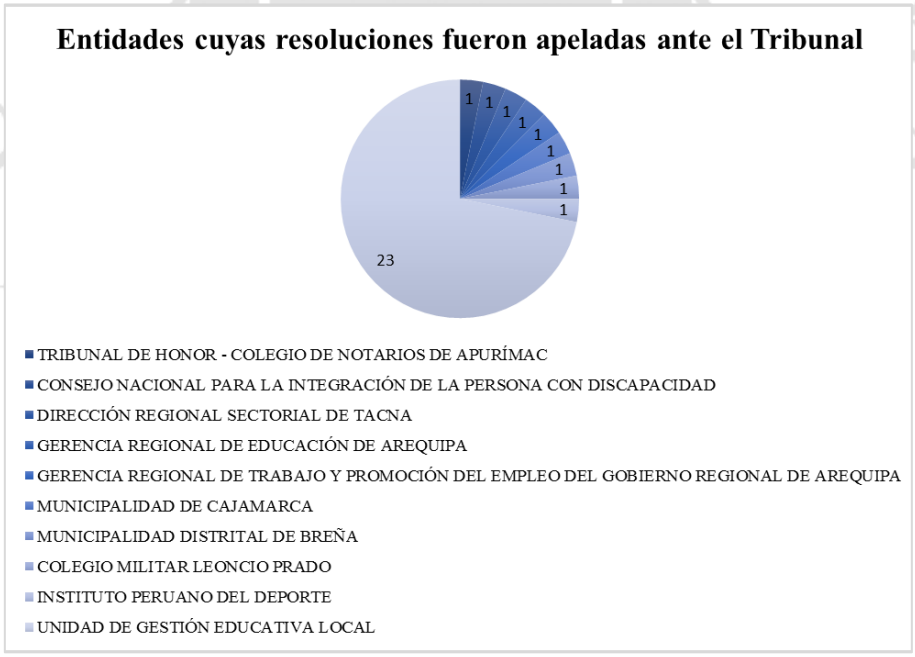

Figura 7

Gráfico en el que se verifica qué entidades estatales han presentado resoluciones que fueron apeladas ante el Tribunal de Transparencia y Acceso a la Información Pública. En él se aprecia que las Unidades de Gestión Educativas son las que tienen el mayor número de resoluciones apeladas.

3.4. Ejercicio del derecho de acceso a la información pública

El acceso a la información pública está sujeta a un procedimiento sencillo que inicia con una solicitud dirigida al funcionario designado por la entidad. La entidad tiene un plazo determinado para responder y brindar la información, el cual puede ser prorrogado hasta por cinco días adicionales. En caso la entidad no posea la información solicitada debe indicar su ubicación correcta y destino, o denegar el acceso a ella en caso sea de carácter secreto, reservado o confidencial.

Si el solicitante no obtiene respuesta de la entidad dentro del plazo establecido o no queda conforme con la recibida, puede interponer recurso de apelación dentro de un plazo máximo de 15 días hábiles, ante el Tribunal.

El Tribunal solicita a la entidad que le remita sus descargos. Evaluado el caso, puede confirmar, modificar o revocar la decisión de la entidad y en caso declare fundado el recurso de apelación interpuesto por el apelante, ordenará la entrega de la información solicitada.

El pronunciamiento del Tribunal agota la vía administrativa, por lo que en caso el solicitante no esté conforme con lo que ésta haya resuelto puede iniciar un Proceso Contencioso Administrativo o interponer un recurso de Habeas Data. En estos procesos también puede solicitar las medidas cautelares que considere pertinentes.

3.5. Importancia de los portales de transparencia y datos abiertos gubernamentales

La Ley Nro. 27806 -Ley de Transparencia y Acceso a la Información Pública-, publicada en 2002, exigió a las entidades de la Administración Pública que implemente, de manera progresiva y según su presupuesto, la difusión de sus datos generales e información general a través de Portales de Internet. Sin embargo, el Banco Interamericano de Desarrollo publicó el Libro "*El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital*" en el que reporta que en Perú se requieren 8.6 horas para realizar un trámite y sólo el 29% de los ciudadanos completa sus trámites en una sola visita al organismo a cargo, sólo el 17% de los trámites que se realizan con el Estado son

considerados fáciles por efectuarse en una sola interacción y en menos de dos horas. (B. R. A. F. P. P. M. V. H. A. S. P. N. E. E. L. L. S. F. P. Roseth, 2018, pp. 48–54)

Con el objetivo de brindar un servicio de mayor calidad a los ciudadanos mediante la digitalización en el sector público, el 13 de setiembre de 2018 se promulgó el Decreto Legislativo que aprueba la Ley de Gobierno Digital -Decreto Legislativo N° 1412- en la que queda establecido que la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno Digital, es el ente rector en materia de gobierno digital y el encargado de promover la apertura de los datos de calidad y la implementación de comités de Gobierno Digital en cada unidad ejecutora y Gobernanza de Datos por parte de la Administración Pública. De este modo, el gobierno busca regular los procesos de recopilación, procesamiento, publicación, almacenamiento y apertura de los datos como estrategia para asegurar la transparencia en la gestión pública.

Esta ley considera entre sus principios rectores el de datos abiertos por defecto; es decir que asume que los datos se deben encontrar abiertos y disponibles a favor de los ciudadanos, y no deben vulnerar el derecho a la protección de datos personales de terceros; ahora bien, es de advertir que, en caso de duda en la aplicación de este principio, el ente encargado deberá resolver la cuestión.

Para que se cumplan los objetivos de un Gobierno Digital es necesario que existan los siguientes campos de acción: tecnologías digitales, identidad digital, servicios digitales, datos, interoperabilidad, seguridad y arquitectura digital.

Conforme a la norma, un dato es aquel activo estratégico y elemento sustancial para la existencia de una verdadera transparencia en un gobierno abierto, digitalizado, que, debido a su buen uso, lucha de manera más efectiva contra la corrupción. Además, la ley señala que para cumplir con estos objetivos debe existir una Gobernanza de Datos, la cual requiere de una Infraestructura Nacional de Datos debidamente provista de un conjunto de políticas, normas, procesos etc., para promover la adecuada recopilación, procesamiento, publicación y almacenamiento de los datos que son administrados por las entidades públicas.

CAPITULO IV

ANÁLISIS DE LA JURISPRUDENCIA PERUANA EN LA QUE SE PRIORIZA EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES SOBRE EL DERECHO DE ACCESO A LA INFORMACIÓN

A partir del análisis de los siguientes casos, se verificará como es que la autoridad competente en Perú da a conocer soluciones ante las controversias en las que el derecho de protección de datos personales se confronta con el derecho de acceso a la información.

4.1. Crítica a la Opinión Consultiva Nro. 025-2021-JUS/DGTAIPD que establece que el padrón electoral, a pesar de ser un documento público, luego de la etapa de sufragio del proceso electoral, no puede ser divulgado para evitar la afectación a la intimidad de los titulares de los datos personales

La segunda vuelta de las elecciones presidenciales de 2021 en Perú, en las que participaron Keiko Fujimori, por el partido político Fuerza Popular, y Pedro Castillo, por el partido político Perú Libre, trajo consigo una serie de controversias en torno a requerimientos de acceso a la información a la autoridad electoral, incluso hubo pronunciamientos enfrentados por parte de diferentes autoridades del Estado.

Los resultados de esos comicios fueron objeto de varios cuestionamientos, ya que Fuerza Popular señalaba que existía un número elevado de actas que habían sido declaradas nulas por los Jurados Electores Especiales, debido a errores de los miembros de mesa al momento de llenar el Acta Electoral, pues consignaron que el número de electores que efectivamente votaron en la mesa de sufragio era menor que el de votos escrutados.

La consecuencia inmediata de declarar un Acta Electoral nula, es que todos los votos emitidos en esa mesa dejan de ser considerados en el conteo general y, por lo tanto, se desconocería la voluntad electoral de los ciudadanos que acudieron a dicha mesa.

Tomemos como ejemplo el caso del Acta Electoral Nro. 033779-93-A, en la que los miembros de mesa, por un error material, agregaban la siguiente información en el Acta Electoral:

<table>
<tr>
<td rowspan="2">Número total de electores hábiles en el acta de instalación: 300</td>
<td>Votos a favor d Perú Libre: 53
Votos a favor de Fuerza Popular: 152
Votos en blanco: 84
Votos nulos: 11</td>
<td rowspan="2">Total de ciudadanos que votaron: 216
Total de cédulas no utilizadas: 84</td>
</tr>
<tr>
<td>Votos emitidos: 300</td>
</tr>
</table>

Como vemos, el error que generó que esta Acta Electoral fuera declarada nula, yace en que los miembros de mesa, en vez de llenar el casillero de votos en blanco con “cero”, lo llenaron con la información correspondiente al total de cédulas de votación no utilizadas (84).

Ante esta situación, se hacía necesario verificar la “Lista de Electores” (Padrón Electoral), documento en posesión de la Oficina Nacional de Procesos Electorales (ONPE) para, de esta forma, confirmar el número correcto de electores que efectivamente sufragaron en mesa y así hacer respetar sus votos y evitar que se declarasen nulos, reduciendo significativamente la cantidad de votos a favor de los partidos Fuerza Popular y Perú Libre.

Lo antes referido sucedió con varias Actas Electorales a nivel nacional, influyendo directamente en la suma total de votos asignados a cada agrupación política y al número de votos nulos; lo que, a su vez, a criterio de muchos, acarreó además la adulteración de la voluntad popular con el desconocimiento de sus votos.

La nulidad de estas actas sería determinada por los respectivos Jurados Electorales Especiales a nivel nacional, por ello es que el partido Fuerza Popular solicitó a la ONPE que le proporcionase copia certificada de las “Listas Electorales” (Padrón Electoral) por mesa de sufragio, a nivel distrital, provincial, regional y en el extranjero, suscritas y utilizadas en la segunda elección presidencial. Con ellas, sostenían, podrían acreditar ante esta autoridad y, en su oportunidad, ante el Jurado Nacional Electoral (en segunda

instancia) la necesidad de que se verifique la existencia de un error en el llenado del Acta Electoral; lo cual podía confirmarse, además, por contraste con el número total de electores que asistieron a votar en cada mesa cuya Acta Electoral fue observada o apelada.

Sin embargo, las autoridades electorales indicaron que las "Listas Electorales" (Padrón Electoral) son documentos que contienen información con datos sensibles que están protegidos por el inciso 5. del articulado 2 que se encuentra en la Ley Nro. 29733 -LPDP, y que en ellos se podría apreciar la declaración de discapacidad de un ciudadano, por ejemplo, así como su huella dactilar, en caso haya asistido a votar, por lo que este padrón no podía ser revelado ni al público ni, tampoco, a las mismas autoridades que resuelven este tipo de controversias.

Los diversos Jurados Electorales Especiales a nivel nacional y el Jurado Nacional de Elecciones (JNE), en audiencias públicas transmitidas en vivo por el portal de YouTube de la entidad, negaron la exhibición del Padrón Electoral por considerarlo un documento que contiene información privada y porque el proceso electoral carece de una etapa probatoria en la que se pueda verificar el referido documento. Sin embargo, uno de los integrantes del Jurado Nacional Electoral, Sr. Luis Carlos Arce Córdova emitió en todas y cada una de las Resoluciones, un voto en minoría. Tal es el caso de la Resolución Nro. 0636-2021-JNE de fecha 16 de junio de 2021, en la que dicho magistrado argumenta que el rol del Jurado Nacional Electoral es de carácter constitucional y tiene, por tanto, la obligación de garantizar que las elecciones presidenciales sean limpias, transparentes y que reflejen, por tanto, la verdadera voluntad popular de los ciudadanos; en tal sentido debían asegurarse de que los comicios no tengan ningún cuestionamiento, a fin de reforzar la estabilidad democrática del próximo presidente electo. Siguiendo esta lógica, el JNE estaría plenamente facultado a revisar los errores numéricos en los actos de escrutinio sobre mesas de sufragio, tal y como lo establecen los artículos 176 y 185 de la Constitución, y, por lo tanto, sería válido que se tuviera a vista la "Lista de electores" (Padrón Electoral) de la mesa de sufragio en cuestión en cada caso, para poder pronunciarse respecto de la existencia o no de un error numérico en el llenado del Acta Electoral, motivo de solicitud de nulidad de este último documento. Ahora bien, cabe advertir que el Padrón Electoral es el único documento con el que es posible verificar el número de votantes que acudieron al acto de sufragio e incorporaron su firma y huella, de modo que, con un simple cotejo con el Acta Electoral, podría determinarse

fehacientemente el número real de electores y se dilucidará cualquier duda al respecto. (Resolución Nro. 0636-2021-JNE, 2021)

En esta coyuntura, fueron emitidas opiniones discrepantes entre diversas autoridades gubernamentales. Por un lado, el entonces Defensor del Pueblo, Sr. Walter Gutiérrez, indicó que el Padrón Electoral es público, por lo que debe ser exhibido para respetar la transparencia de las elecciones presidenciales.

Por otro lado, el Registro Nacional de Identificación y Estado Civil -RENIEC- efectuó una consulta a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (la Dirección) sobre la posibilidad de proporcionar la información contenida en el Padrón Electoral ante solicitudes de acceso a la información pública. Al respecto RENIEC precisa que con anterioridad el Tribunal de Transparencia y Acceso a la Información Pública le ordenó entregar la información que contiene el Padrón Electoral, siempre y cuando se cumpla con efectuar un procedimiento previo de tachado de los datos confidenciales relacionados con el derecho a la intimidad personal y familiar de terceros, es decir, de la fotografía y firma digitalizada, la declaración de discapacidad, domicilio e impresión dactilar.

La Dirección absolvió la consulta efectuada por RENIEC mediante Opinión Consultiva Nro. 025-2021-JUS/DGTAIPD de fecha 26 de julio de 2021, indicando que el Padrón Electoral contiene información personal y para evaluar la publicidad de este documento se tiene que tener en cuenta el principio de finalidad para el tratamiento de estos datos personales, señalando que el artículo 197 de la Ley N° 26859 -Ley Orgánica de Elecciones- (LOE) indica expresamente que el Padrón Electoral es público. Según la interpretación de la Dirección, tal carácter público sólo lo es con la finalidad de que los partidos políticos o ciudadanos puedan reclamar el error u omisión de sus datos o la eliminación de los ciudadanos fallecidos en el Padrón Electoral, por lo que, una vez vencido el periodo de tachas y observaciones, se tendrá el Padrón Actualizado, dándose por agotada y cumplida la finalidad establecida en el artículo 201 de la LOE. En efecto, luego de la etapa de tachas y observaciones, el Padrón Electoral aprobado se convierte en una lista de datos personales de ciudadanos mayores de edad a nivel nacional, cuya entrega a raíz de una solicitud de acceso a la información pública sólo podrá efectuarse contando con el consentimiento previo de estos ciudadanos. En tal sentido, la Dirección

utiliza al principio de finalidad contemplado en el artículo 6 de la LPDP para determinar que el Padrón Electoral, si bien es un documento público, únicamente lo es durante la etapa en la que los ciudadanos o partidos políticos pueden presentar tachas u observaciones, y una vez que esta etapa ha concluido, habiéndose cumplido con la finalidad para la que fue creado, no es publicable; en efecto, proporcionar este documento equivaldría a publicar datos personales allí contenidos poniendo en peligro el derecho a la protección de datos personales, lo que además facilitaría que traten estos datos sin el consentimiento previo de sus titulares y, por lo tanto, puedan darse fácilmente conductas delictivas. (*Opinión Consultiva Nro. 025-2021-JUS/DGTAIPD,* 2021)

Lo más sorprendente y contradictorio de la Opinión Consultiva de la Dirección es que en anteriores casos, esta entidad sí permitió la entrega del Padrón Electoral, exigiendo que previamente se efectúe un proceso de disociación de la información protegida, permitiendo inclusive que se elaboren versiones públicas del Padrón Electoral.

De los hechos antes referidos se constata que el proceso electoral para elegir al nuevo presidente del Perú en los comicios de 2021 se caracterizó por generar la polarización de posturas respecto del acceso al Padrón Electoral, así como sobre el carácter público o privado de este documento.

Si bien el principio de finalidad se entiende en relación con la previsibilidad y el control del titular respecto de los datos al que se brinda acceso, así como en cuanto al poder de presentar oposición al tratamiento de esta información en caso sea utilizada para fines diferentes para los que fueron otorgados, nos preguntamos si es que el principio de finalidad debe ser interpretado como una limitación absoluta y si es que, en base a este principio, corresponde priorizar la protección de datos personales y restringir otros derechos fundamentales tales como el derecho de acceso a la información pública, determinante para hacer respetar la voluntad popular en un proceso de elección presidencial. Y en el caso en el que el derecho de protección de datos personales se contraponga al derecho de acceso a la información pública, ¿Qué criterios cabría aplicar para limitar uno u otro derecho?

Damos respuesta a estas preguntas en base al principio de proporcionalidad, pues estamos frente a dos derechos constitucionales que en ocasiones pueden contraponerse:

por un lado, el derecho a la protección de datos personales (inc. 4 del artículo 2 de la Constitución) y, por el otro, el derecho al acceso a la información pública (inc. 5 del artículo 2 de la Constitución).

Ante esta situación de conflicto, lo que corresponde es aplicar una solución que, según criterios adecuados, disponga priorizar unos derechos por sobre otros. Por lo tanto, la pregunta es ¿Bajo qué criterios es que se puede justificar la priorización de un derecho sobre otro? La respuesta está en aplicar el denominado *balancing test*, test de ponderación de derechos o principio de ponderación, figura contemplada en el último párrafo del artículo 200 de la Constitución, y que ha aplicado el Tribunal Constitucional peruano en varias otras ocasiones, con lo que ha logrado la limitación de un derecho fundamental en base al principio de razonabilidad, siempre a fin de garantizar un fin legítimo que también tiene rango constitucional. (Sentencia Exp. 2235-2004-AA/TC, 2005, Fundamento 6)

Conforme lo señala el Tribunal Constitucional, el principio de ponderación incluye a su vez la aplicación de los siguientes principios: (*i*) idoneidad, (*ii*) necesidad y (*iii*) ponderación o proporcionalidad en sentido estricto. Estos últimos se deben aplicar en orden, empezamos con el principio de idoneidad o adecuación para ver si es que la limitación del derecho resulta acertada para lograr tutelar el derecho constitucional. Una vez que se supere este primer test se procederá a analizar si la restricción de este derecho es necesaria para lo que se debe verificar si es que existen otros medios para alcanzar el mismo fin y evitar la restricción de otro derecho. Una vez que se haya superado este segundo test se procederá con el análisis de la ponderación en sentido estricto y determinar el valor de los derechos que se encuentran en conflicto.

La aplicación de este procedimiento permite responder a la interrogante de si es que se debe o no limitar el acceso a determinada información que está en posesión de una entidad del Estado, así como si es que dicha limitación lesiona o no otros bienes jurídicos protegidos en la Constitución.

En el caso en concreto, consideramos que la finalidad a la que debe obedecer este test de ponderación es a respetar la voluntad popular para la elección del presidente del Perú, derecho protegido en el inciso 17 del Art. 2, así como el Art. 111 de nuestra Constitución. Para ello tendría que haberse brindado acceso al Padrón Electoral, documento en posesión

de la ONPE. Por lo tanto, cabe que nos preguntemos si es correcto que esta entidad estatal, así como la Dirección, puedan impedir la exhibición del Padrón Electoral, privilegiando con ello el derecho a la protección de datos personales por sobre el de acceso a la información pública.

Aplicando el procedimiento del test de ponderación, apuntamos que:

En cuanto al análisis de *idoneidad*:

Al respecto, cabe preguntarnos si es que es la decisión de la ONPE y de la Dirección de no proporcionar el Padrón Electoral, expresada a través de la Opinión Consultiva Nro. 025-2021-JUS/DGTAIPD, ha sido una medida adecuada para lograr la finalidad indicada previamente. Consideramos que no, pues justamente para lograr la finalidad establecida habría que permitir la publicación del Padrón Electoral.

En cuando al análisis de *necesidad*:

En este punto nos debemos preguntar si es que existen otros medios alternativos que pudieron ser utilizados para evitar la restricción al derecho de poder acceder a la información pública al no ser secreta. Consideramos que la ONPE y la Dirección pudieron adoptar otras medidas; por ejemplo, hacer entrega del Padrón Electoral luego de haber pasado por el procedimiento de disociación de aquellos datos calificados como privados o, simplemente, innecesarios de exponer, tales como la firma, domicilio y huella dactilar de los votantes.

Es de notar que el objetivo del proceso de desclasificación de información es poner a disposición de la ciudadanía aquella información que no configure riesgo de exposición o afectación de la privacidad, priorizando siempre el principio de publicidad de la información que tiene determinada entidad estatal. Es de notar que la publicación del Padrón Electoral no requiere del consentimiento previo de los titulares de los datos, ya que conforme a lo establecido en el inciso 2 del artículo 14 de LPDP, nos hallamos ante datos personales contenidos y destinados a fuentes accesibles para el público.

En cuanto al análisis de *ponderación o proporcionalidad en sentido estricto*:

> En este punto debemos asignar un peso a cada derecho en conflicto, tendiendo en cuenta la finalidad constitucional que se pretende proteger. Para ello, debemos aplicar el principio de ponderación conforme a la cual refiere que mientras más incremento tenga la afectación en el ámbito de los derechos que protegen los datos personales, también aumentaría el grado de satisfacción o cumplimiento del derecho al acceso a la información pública.

Una vez aplicado el principio de ponderación es que podemos ver que en el caso materia de análisis se debió privilegiar el derecho de acceso a la información pública, ya que corresponde transparentar información que sólo puede ser proporcionada por una entidad estatal, especialmente tomando en cuenta que la única forma de que hacerlo era con el acceso al Padrón Electoral. La ONPE debió proporcionar el referido documento, y en caso de riesgo de vulneración de derechos de datos personales de determinados ciudadanos, debió someter el Padrón Electoral a un proceso de disociación y tener una versión pública accesible a la población o a las otras entidades públicas que requieran verificar este documento para resolver controversias. Ello, toda vez que la misma Dirección ha establecido, en su Informe Jurídico N° 002-2018-JUS/DGTAIPD que de existir algún extremo en los documentos que a criterio de la respectiva entidad debería de ser vista por la sociedad por estar presente en las excepciones puestas en la normativa vigente, deberán de darse a conocer los principios de publicidad y de divulgación de carácter máximo, de tal manera que se de a conocer a la persona que lo solicite aquella parte de información que no estuviera impedida por la condición prescrita. (Dirección de Transparencia y Acceso a la Información Pública y Protección de Datos Personales, 2018)

Mediante Opinión Consultiva N° 037-2019-JUS/DGTAIPD, la Dirección ha indicado, en el fundamento 26, que para la difusión de datos personales tendrá que realizarse un ejercicio de ponderación para resguardas sólo aquella información que podría colisionar con la intimidad de los ciudadanos frente al legítimo interés de otros a acceder a la información pública que les permita vigilar el ejercicio del poder por parte de los funcionarios públicos. (*Opinión Consultiva N° 037-2019-JUS/DGTAIPD,* 2019)

A lo antes dicho corresponde añadir que el Tribunal Constitucional advierte que los ciudadanos podemos exigir del Estado la obligación de probar que existe un bien, principio o valor constitucionalmente relevante que justifique que se mantenga en reserva, secreto o confidencialidad determinada información pública. (Sentencia TC Exp. N° 2579-2003-HD/TC, 2004, Fundamento 13)

Asimismo, consideramos que no existe justificación alguna para que la ONPE no haya proporcionado el Padrón Electoral, dado que ni siquiera contaba con un registro que acreditase que el Padrón Electoral era de acceso restringido, conforme lo establece el artículo 21 del Decreto Supremo Nro. 072-2003-PCM -Reglamento de la Ley de Transparencia y Acceso a la Información Pública-.

Consideramos que, adicionalmente, a lo expuesto anteriormente se debe aplicar la "fórmula del peso" propuesta por Alexy y que desarrollaremos ampliamente en el Capítulo VI de la presente investigación .

4.2. Análisis del proceso seguido en contra de la Municipalidad Metropolitana de Lima para que se proporcione la lista de usuarios bloqueados de su perfil oficial de Facebook

Otro caso que causó controversia en Perú fue el que se dio cuando el Sr. José Wilfredo Arrieta Caro solicitó a la Municipalidad Metropolitana de Lima que le brindara la siguiente información: (*i*) la lista completa de los usuarios bloqueados por la Municipalidad en su página oficial de Facebook y (*ii*) los nombres de los funcionarios que administran la página de Facebook de la Municipalidad. La solicitud tuvo su motivo en que la Municipalidad venía bloqueando a usuarios que manifestaban sus críticas a la entidad a través de su portal de en dicha red social.

La Municipalidad respondió al requerimiento indicando que no era posible proporcionar las listas de usuarios bloqueados, la que consideraban confidencial, y omitieron, sin más, el segundo punto de la solicitud.

Ante esta negativa de la Municipalidad, el Sr. José Wilfredo Arrieta Caro interpuso una demanda constitucional de Habeas Data contra la entidad. Mediante sentencia de

fecha 09 de octubre de 2017, puesta también en el Expediente Nro. 14190-2015, el juez constitucional a cargo considera que cualquier tipo de información obrante en los archivos o registros de una entidad pública constituye información de carácter público y, por lo tanto, de libre acceso a quien lo solicite. Así, la Municipalidad estaba obligada a proporcionar la lista de usuarios bloqueados y el nombre de los funcionaros a cargo de administrar la página de Facebook de la Municipalidad. La demanda fue declarada fundada en todos sus extremos.

Coincidimos con la sentencia emitida por el Juez Constitucional, pero consideramos grave que un ciudadano tenga que acudir a un proceso constitucional de Habeas Data para poder dar su ingreso, recién así, a información de carácter público a raíz de la negativa injustificada de la Municipalidad.

Como ha sido precisado, si bien las entidades públicas pueden mantener determinada información bajo reserva, esto sólo puede ser por un plazo determinado. De manera que es de exigir a las entidades públicas que tengan procedimientos internos que fundamenten que determinada información se encuentra clasificada y no puede, por tanto, ser publicada, indicando el plazo de dicha reserva, al cabo del cual ha de proceder la desclasificación respectiva. (Opinión Consultiva Nro. 036-2021-JUS/DGTAIPD, 2021, Fundamento 23)

CAPÍTULO V

DERECHO AL OLVIDO

5.1. Definición

El derecho al olvido es aquél que permite a una persona solicitar la supresión, cancelación o limitación del uso de los datos personales que han estado por un tiempo considerable a disposición de los buscadores de Internet. El titular de este derecho busca con ello limitar el acceso a su información, lo que puede deberse a que ésta sea falsa, caduca, inexacta, o porque considera que el acceso a ella le perjudica de algún modo. Este derecho pretende garantizar el respeto a otros derechos constitucionales, tales como el de igualdad y el de no discriminación de personas; así, cada ciudadano puede continuar con el libre desarrollo de su personalidad, ejercer sin problemas su derecho de trabajo, etc.; sin que, en el presente, continúe padeciendo las consecuencias de actos acontecidos en el pasado, en tanto se encuentren publicados en Internet. (Cabezas Poma, 2020, pp. 470–471)

Como ejemplo de la aplicación de este derecho, podemos plantear el caso las detenciones arbitrarias que efectuaron miembros de la Policía Nacional del Perú y el Serenazgo del distrito de Miraflores a unos jóvenes que fueron a Larcomar para un evento de ciclismo. Estas autoridades argumentaron que los detenidos eran integrantes de una banda criminal denominada “Los malditos de Larcomar”, siendo el caso, sin embargo, que no habían cometido ningún delito. Lo cierto es que se trataba de un error por parte de las autoridades, las que aclararon la situación a los pocos días del acontecimiento. Sin embargo, la noticia de la detención de estas personas, en la que se mostraba sus rostros y su identidad ya había corrido por diversos medios de comunicación. Era importante, como es claro, que el hecho fuera efectivamente “olvidado”.

Otro ejemplo es el de las personas que son grabadas por las cámaras de televisión en situaciones bochornosas mientras se encuentran bajo los efectos del alcohol. Cuando uno de estos vídeos no sólo es publicado en televisión nacional, sino que es difundido y permanece por tiempo indefinido en Internet y en redes sociales, queda a disposición de

miles y miles de usuarios.

La pregunta que se desprende de ambos casos es si es que los protagonistas de los ejemplos anteriores tienen derecho a solicitar que la información que se publicó respecto a los incidentes de los que participaron sea eliminada de los buscadores de Internet en ejercicio del derecho al olvido.

El derecho al olvido se ha desarrollado más ampliamente por los legisladores y tribunales de la Unión Europea, en base a un principio al que han denominado "*principio de minimización de datos*", derecho reconocido, inclusive, dentro de algunos cuerpos legales como el del Consejo de Europa y el de la Unión Europea.

En Perú, el derecho al olvido no es reconocido legalmente, no de forma expresa; sin embargo, el artículo 20 de la LPDP reconoce que el titular de los datos personales tiene derecho a solicitar la supresión de su información, cuando ésta ya no sea necesaria o pertinente para la finalidad para la cual fue recabada.

Por otro lado, el artículo 17 del Reglamento General de Protección de Datos establece que las circunstancias bajo las cuales el responsable del tratamiento de los datos tiene la obligación de atender una solicitud de supresión de datos, atiende los casos en que: *(i)* los datos ya no cumplen con la finalidad para la cual fueron recabados, *(ii)* el titular retira su consentimiento o se opone al tratamiento de sus datos, o *(iii)* cuando exista ley expresa que establezca que determinada información debe ser suprimida.

Para el caso de las entidades públicas, es pertinente señalar que éstas pueden negar la supresión de la información que poseen en el supuesto en que de este modo se proteja derechos de terceros, o si es que al eliminar la información quepa obstrucción de actuaciones judiciales o administrativas en procesos de diversa índole, al desarrollo del control de la salud y del medio ambiente. Por otro lado, las entidades públicas no pueden, en ningún caso, destruir la información que poseen, ésta deberá ser envida al Archivo Nacional para su custodia o posterior destrucción en caso ya no tenga ningún tipo de utilidad pública, todo ello a efectos de que el derecho al acceso a la información pública pueda ser ejercido a plenitud (Artículo 18 de la LTAIP).

El derecho al olvido también tiene límites y excepciones en mérito a las cuales el responsable del tratamiento de datos queda habilitado para no suprimir o limitar el acceso a la información. Estas excepciones se dan cuando, paralelo a un requerimiento de supresión, se ejerce el derecho a la libertad de expresión y de información, cuando estos datos son objeto de gestión para dar cumplimiento a una norma, en casos de emergencia y en el ámbito de salud pública.

5.2. Sujetos y autoridades vinculadas a la aplicación de la legislación de derecho al olvido

Entre los sujetos vinculados al ejercicio del derecho al olvido, tenemos, en primer lugar, al titular mismo, cuyos datos personales se encuentran almacenados en bases de datos o motores de búsqueda que pueden ser de propiedad de un particular o de una entidad pública. Además, precisamos que la información que está contenida en estas bases de datos o motores de búsqueda puede provenir de declaraciones o publicaciones propias del mismo titular, así como de un tercero que informa de algún dato personal del titular en ejercicio de su derecho a la libertad de información o de expresión. Ahora bien, la información publicada debe ser de carácter sensible para que el titular pueda solicitar su eliminación.

Por otro lado, tenemos a la persona natural o jurídica, responsable del tratamiento de los datos personales del titular. Y, por último, a las autoridades que pueden pronunciarse respecto de las controversias, entre ellas, la Dirección General de Protección de Datos Personales. Esta entidad puede, en una instancia administrativa, resolver la reclamación que efectúe el titular. Por otra parte, el Juez Constitucional puede conocer, a través de un proceso de Hábeas Data, la demanda de un titular.

5.3. Caso Mario Costeja Vs. Google España

El derecho al olvido fue aplicado por primera vez en España en 2014, específicamente en el caso de Google España S.L, Google Inc v. Mario Costeja Gonzáles.

Ocurrió que el Sr. Mario Costeja Gonzáles vio embargados bienes suyos en distintos procesos judiciales, debido a deudas que tenía con la seguridad social española, ello en la

década de 1990. El hecho del embargo fue cubierto como noticia por el diario La Vanguardia en un par de artículos. Luego de un tiempo, el Sr. Costeja logró pagar sus deudas; sin embargo, trascurridos diez años, su nombre: Mario Costeja Gonzáles, arrojaba en Google, resultados que derivaban en enlaces de la página Web del diario La Vanguardia, con los artículos periodísticos a propósito de sus deudas y procesos judiciales. Debido a ello, el Sr. Costeja presentó una denuncia contra el referido periódico y en contra de Google España.

La denuncia se basaba en el hecho de que las controversias derivadas de las deudas del Sr. Costeja ya habían sido resueltas y cualquier referencia adicional a ellas era no sólo irrelevante, sino efectivamente perjudicial para su reputación. Por lo tanto, solicitó que el diario La Vanguardia retirara los artículos y que Google eliminara de sus motores de búsqueda los enlaces que estaban referidos a sus deudas.

La Agencia Española de Protección de Datos (AEPD) desestimó la denuncia en contra de La Vanguardia, considerando que, en su calidad de editora, había publicado legalmente la información en ejercicio de su derecho de libertad de información. Sin embargo, la AEPD sí estimó la denuncia respecto de Google pues consideró que, cuando se efectúa la búsqueda de información en Internet, Google indexa enlaces web para dar contenido a los resultados de estas búsquedas y, al hacerlo, se hace responsable del tratamiento de datos, más allá del rol del diario La Vanguardia, titular del sitio web objeto de indexación.

Finalmente, el Tribunal de Justicia de la Unión Europea (TJUE) dictaminó que la legislación de la Unión Europea (UE) se aplica a los operadores de motores de búsqueda si tienen una sucursal o filial en un Estado miembro, incluso si el servidor que procesa los datos se encuentra físicamente fuera de Europa. (*Sentencia del Tribunal de Justicia de 13 de mayo de 2014,* 2014)

La novedad de esta sentencia brindó reconocimiento al derecho al olvido, con sustento en la Directiva de Protección de Datos; asimismo, abre la posibilidad de suprimir información de motores de búsqueda de internet, aunque dicha información sea veraz y lícita y permanezca en la web que publicó la información originalmente.

Como vemos, no se trata de eliminar la información original sino más bien de limitar

el acceso a ella. Por otro lado, la sentencia establece que debe hacerse un ejercicio de ponderación equilibrada al momento de resolver una controversia en relación a suprimir información de una persona. Para ello, indica que se debe analizar la naturaleza de la información que se pretende suprimir y verificar si está referida a la vida privada del titular o si trata temas de interés público que ameritan su disponibilidad ante la ciudadanía.

5.4. Análisis y crítica al caso Google Perú S.R.L.

En Perú, la situación fue distinta a la referida con el caso anterior. El caso bajo análisis se inició en 2009, cuando un ciudadano fue denunciado anónimamente por el delito de contra el pudor en la modalidad de pornografía infantil. La correspondiente Fiscalía Penal abrió investigación e incluso formalizó su denuncia ante el Quinto Juzgado Penal de Lima, el mismo que en 2012 declaró sobreseída la causa, dado que no se acreditaba la comisión del delito, y ordenó que se anulasen todos los antecedente penales y judiciales de este ciudadano en relación al proceso.

Una vez concluido el proceso penal, el ciudadano solicitó al Juez Penal que ordene a Google Perú S.R.L la eliminación en su motor de búsqueda, de toda información o noticia relacionada al caso penal archivado. Google Perú S.R.L respondió al juzgado indicando que el motor de búsqueda de la plataforma de Google era administrado por Google Inc., empresa constituida y domiciliada en Estados Unidos de América.

Paralelamente, el ciudadano utilizó la herramienta de Google denominada "*quitar o actualizar información obsoleta*" para solicitar la eliminación de su información. Google respondió a esta solicitud indicándole que se pusiera en contacto directo con el propietario del sitio web que publicó las noticias referidas a la denuncia penal.

El 24 de agosto de 2015, el ciudadano presentó una solicitud de procedimiento trilateral de tutela ante la Dirección General de Protección de Datos Personales de Perú (DGPDP). Esta autoridad declaró fundado el reclamo mediante Resolución Directoral Nro. 045-2015-JUS/DGPDP de fecha 30 de diciembre de 2015; asimismo, ordenó a Google (bajo la personería de Google Inc. o de Google Perú S.R.L) que bloquease el acceso a los datos personales del reclamante (sus nombres y apellidos), así como de toda información o noticia relacionada con el proceso sobreseído que apareciera en los

resultados de sus motor de búsqueda, ello, para impedir que esta información quedase disponible para sucesivos tratamientos de búsqueda e indexación. Asimismo, la DGPDP impuso a Google Perú una multa de 35 UIT´s (Unidades Impositivas Tributarias), que al 2015 ascendían a S/ 134,750, debido a que no se atendió la solicitud del reclamante y se desconocieron sus derechos de cancelación y oposición. (*Resolución Directoral Nro. 045-2015-JUS/DGPDP*, 2015)

Google Perú S.R.L presentó un recurso de reconsideración a la Resolución, argumentando que:

- Aunque se notificó válidamente a Google Perú SRL en Lima, no se hizo lo propio con Google Inc. en el Estado de California, en los Estados Unidos, a sabiendas que Google Perú SRL y Google Inc. eran dos personas jurídicas distintas.

- Las notificaciones dirigidas Google Inc. que fueron hechas en el domicilio de Google Perú, en Perú, son nulas de pleno derecho, por lo que contravendrían el debido proceso impidiendo que Google Inc. pudiera ejercer su derecho de defensa.

El recurso de reconsideración presentado por Google Perú S.R.L fue declarado infundado por la DGPDP.

A diferencia de lo ocurrido en el caso contra Google España, el ciudadano peruano buscaba que se retire del buscador de Google las publicaciones periodísticas referidas a un proceso penal que se llevó contra él por delito contra el pudor en la modalidad de pornografía infantil; no se trataba de la eliminación de información referida a deudas.

Otra diferencia importante, y que conllevó una serie de críticas, es que la legislación peruana no regula expresamente el derecho al olvido. La DGPDP hizo una interpretación extensiva del derecho a la autodeterminación informativa y del artículo 20 de la LPDP, que regula el derecho del titular a la eliminación de información personal suya, por solicitud dirigida al responsable del tratamiento la supresión en caso los datos sean parcial o totalmente inexactos, incompletos, o dejen de ser relevantes para cumplir con la finalidad para la cual fueron recopilados en principio.

La LPDP no permite expresamente que el titular de los datos pueda solicitar la eliminación de la información cierta que fue publicada en base al ejercicio de la libertad de expresión y de información de los medios de comunicación. De hecho, la noticia de la denuncia penal fue cubierta en su oportunidad en base a datos ciertos.

5.5. Derecho a la privacidad Vs. derecho de acceso a la información de interés público, y derecho a la libertad de expresión e información

Al aplicar el derecho al olvido se prioriza el derecho de privacidad de la persona por sobre otros derechos constitucionales, como el de acceso a esta información, así como a la libertad de expresión y de información. Estos últimos, como es bien sabido, son esenciales como principios de transparencia en bien de la democracia.

Habida cuenta todo lo expuesto, consideramos que en el caso en el que una autoridad tenga que decidir sobre controversias referidas al derecho al olvido debería sopesar los derechos constitucionales que se contraponen, por lo que necesariamente debe aplicar el *balancing test*, o test de ponderación de derechos al que nos hemos referido antes con detalle. Asimismo, sostenemos que es necesaria la aplicación de los principios de idoneidad, necesidad y proporcionalidad. De este modo, la autoridad también puede analizar a detalle el origen y contenido de la información materia de controversia, a efectos de verificar si es que esta carece de relevancia pública; de lo contrario la información debía de permanecer accesible a los ciudadanos.

Es necesario señalar que, en la actualidad, el flujo de información en Internet no se limita al de los motores de búsqueda de Google; existen otros muchos buscadores a disposición de los usuarios, como Altavista, Yahoo, Bing, entre otros. La información de un ciudadano como el que se enfrentó a Google en Perú podría ser encontrada en cualquiera de estos otros buscadores. De manera que ¿Por qué solicitar a Google que elimine su información, y no a los demás buscadores?

Esta situación nos lleva a reconocer que, dentro del panorama de las redes sociales como Twitter, Instagram, Facebook, LinkedIn, entre otras, también se acumula enorme cantidad de información por segundo, a la que cualquier otro usuario podría tener acceso e incluso podría descargar y almacenar en una memoria cualquiera.

También podríamos referirnos a las veces en que usuarios de WhatsApp reenvían videos íntimos de celebridades a sus amigos, a menudo a través de grupos amplios. Los mensajes pueden, en todo caso, llegar a miles de personas en cuestión de minutos, sin que el titular de la información pueda identificar y requerir a los usuarios que eliminen la información privada que les ha sido compartida y que tienen almacenada en su celular.

Entonces nos preguntamos ¿Hasta qué punto es válido el derecho al olvido si es que sólo lo aplicamos a buscadores como Google? ¿El siguiente paso será también eliminar información en los demás buscadores, incluyendo, además, a redes sociales?

CAPITULO VI

EL PRINCIPIO DE PONDERACIÓN COMO MÉTODO PARA ENCONTRAR EL BALANCE ENTRE EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES

Como hemos explicado a lo largo del presente trabajo, existen casos en los que las distintas autoridades competentes, en muchas ocasiones de manera injustificada, priorizan la protección de la privacidad personal en mérito al derecho de protección de datos personales vulnerando otros derechos que también gozan de protección constitucional como el derecho de acceso a la información pública, el de libertad de información y de expresión.

Por ello, consideramos muy importante que las autoridades que sean competentes para dilucidar este tipo de controversias apliquen un método objetivo que les permita encontrar un equilibrio en entres los derechos que se contrapongan entre sí. En ese sentido, consideramos que el método objetivo que debe aplicarse es el principio de ponderación de derechos. Así, toda entidad pública al resolver las solicitudes de acceso a la información o cuando tengan que determinar si cierta información debe ser eliminada de los motores de búsqueda de alguna página web emplee el principio de ponderación de derechos, siendo además indispensable que siempre se analice a detalle el tipo de información que está en controversia.

Conforme vamos a desarrollar en el presente capítulo el principio de proporcionalidad consiste en examinar el tratamiento diferenciado entre dos derechos constitucionales, tomando en cuenta la finalidad del tratamiento diferenciado, con la aplicación de tres subprincipios:

(i) Idoneidad,
(ii) Necesidad y
(iii) Ponderación o proporcionalidad en sentido estricto.

Hacemos presente que el principio de proporcionalidad ha sido ampliamente desarrollado por el jurista y filósofo alemán Robert Alexy y proponemos su utilización pues además es el principio que viene utilizando el Tribunal Constitucional peruano para resolver la colisión de derechos. (ESPINOSA-SALDAÑA BARRERA Eloy, 2018, p. 2)

6.1. Sobre los métodos de argumentación jurídica

Debemos iniciar explicando que el principio de ponderación de derechos es un método de argumentación jurídica que nos da el camino para llegar a conclusiones válidas al aplicar e interpretar el derecho en la toma de decisiones administrativas o judiciales. Así se puede afirmar que los fundamentos de la argumentación jurídica se basan en la subsunción y en la ponderación dependiendo si es que estamos frente a reglas o principios; (Bernal Pulido, 2006, pp. 51–53) conforme desarrollamos a continuación:

6.1.1. Las reglas

Las reglas son normas que se van a cumplir o no, en caso la norma tenga validez entonces se ordena hacer exactamente aquello que la norma exige, ni más ni menos. Es así como las normas tienen valores en el ámbito fáctico y jurídico convirtiéndose en *mandatos definitivos*.

Para argumentar si determinada regla se aplicó o no, se utiliza el método de subsunción, el cual consiste en verificar que se hayan cumplido los enunciados detallados en el supuesto de hecho de la regla para entonces aplicar la respectiva consecuencia jurídica. Por lo que en caso suceda lo descrito en el supuesto de hecho (A) entonces se aplica definitivamente la consecuencia jurídica (B). Un claro ejemplo del método de subsunción en una regla es la imposición de una multa por cruzar una intersección cuando el semáforo está con luz roja, al respecto el Texto Único Ordenado del Reglamento Nacional de Tránsito – Código de Tránsito, aprobado por el Decreto Supremo Nro. 016-2009-MTC, indica lo siguiente:

(A)	**Supuesto de hecho**	Cruzar una intersección o girar, estando el semáforo con luz roja y no existiendo la indicación en contrario.
(B)	**Consecuencia jurídica**	Imposición de multa equivalente a 12% UIT.

Como notamos en el ejemplo antes expuesto, en caso se verifique que una persona esté conduciendo un vehículo y cruce una intersección mientras la luz del semáforo esté en color rojo, inmediatamente se aplica la Consecuencia Jurídica (B), por lo que a este conductor se le aplicará una multa equivalente al 12% de la UIT.

A lo antes dicho, debemos añadir que en caso dos o más reglas entren en colisión o contradicción la solución está en introducir excepciones a una de esas reglas en conflicto para declarar la invalidez de una de ellas aplicando los preceptos de *"ley posterior deroga ley anterior"* y *"ley de rango superior prevalece sobre ley de rango inferior"*.

6.1.2. Los Principios

A diferencia que, con las reglas, los principios son normas que ordenan que algo se realice en la mayor medida posible, de acuerdo con las posibilidades fácticas y jurídicas. Para Alexy los principios son considerados como *mandatos de optimización* y que por lo tanto pueden ser satisfechos en diferentes grados o niveles.

A diferencia de las reglas la argumentación jurídica y el método a aplicar ante la colisión de dos principios es diferente, ya que se al aplicar mandatos de optimización se busca efectuar el uso más amplio y extenso de los principios en controversia y la consecuencia jurídica de esta optimización no tiene una consecuencia jurídica exacta, por el contrario, al tratarse de principios intrínsecos a derechos constitucionales tendrán consecuencias jurídicas de carácter amplio y extendido. (Carbonell, 2021)

Ahora bien, ¿Cómo se resuelven las controversias en la que dos principios colisionan? Cuando esto sucede, como lo hemos dicho anteriormente, el método de argumentación jurídica a aplicar es el de la ponderación, precisando que con la ponderación no se eliminará a ningún principio; si no por el contrario se optimizará la aplicación de uno de ellos en el caso en concreto siguiendo esta premisa: "*Cuanto mayor es el grado de insatisfacción o de afectación de uno de los principios, tanto mayor debe ser la satisfacción del otro*."

6.2. El principio de ponderación y su estructura

Alexy nos explica que la optimización de derechos que se realiza a través del principio de proporcionalidad tiene que estar legitimado y hay que otorgarle una medida de racionalidad, y para ello Alexy crea una estructura al principio de ponderación que básicamente está compuesta por dos leyes: (i) "ley material de la ponderación" y (ii) "ley epistémica de la ponderación"; estas dos leyes se reflejan a su vez en una fórmula que este autor denomina la "fórmula del peso". (Alexy, 2019a)

6.3. El "principio no satisfecho" y el "principio contrario"

Para entender a la fórmula del peso que a su vez está compuesta por la ley material de la ponderación y la ley epistémica de la ponderación, primero debe quedar claro que la ponderación requiere de dos principios o derechos que colisionan entre sí, a uno de estos principios lo llamaremos "principio no satisfecho" y al segundo "principio contrario".

El "principio no satisfecho" es un derecho de defensa que ha sido intervenido o vulnerado, se le ha restringido; y lo que se pretende con la fórmula del peso es medir y asignar un valor a esta intervención o a esa "no satisfacción". En adelante a este derecho o principio no satisfecho le denominaremos **Pi**.

Por otro lado, el segundo principio es un "principio contrario" y se trata de un derecho de protección que refleja un actuar positivo, este principio es uno que si ha sido satisfecho. En adelante a este derecho o principio contrario le denominaremos **Pj**.

Los dos principios en colisión antes detallados son analizados y valorados por la "ley material de la ponderación" y la "ley epistémica de la ponderación" como explicamos a continuación. (Alexy, 2019a)

6.4. La "ley material de la ponderación"

La "ley material de la ponderación" indica que: *"Cuanto mayor sea el grado de no satisfacción o restricción de uno de los principios, tanto mayor deberá ser el grado de la importancia de satisfacción del otro"*.

Esta ley nos permitirá otorgar un valor a los subprincipios de idoneidad y de necesidad, para lo cual debemos seguir los siguientes tres pasos: (Alexy, 2019a)

Primer paso:
Trata de definir el grado de la no satisfacción o de afectación de uno de los principios.

Segundo paso:
Trata de buscar la satisfacción del principio que juega en sentido contrario.

Tercer paso:
Trata de verificar si la importancia de la satisfacción del principio contrario justifica la restricción o la no satisfacción del otro.

6.5. La "ley epistémica de la ponderación"

La "ley epistémica de la ponderación" indica que: *"Cuanto mayor sea una intervención en un derecho fundamental, tanto mayor deberá ser la certeza de las premisas que fundamentan la intervención"*.

Esta ley se denomina epistémica porque, con esta ley buscaremos encontrar criterios de verdad que justifiquen la intervención en un derecho, entonces esta ley nos permitirá evaluar el grado de seguridad de la ocurrencia de la intervención o medida examinada en el caso en concreto según experiencias pasadas ya sea para la no realización de **Pi** y la realización de **Pj**. La finalidad de esta ley es expresar tanto la fuerza de defensa como la de ataque ante la creciente incertidumbre de las premisas que soportan cada uno de los principios. Los criterios con los que se aplique esta ley pueden ser relacionados entre si

para fundamentar un resultado y siempre deberán ser consecuentes con líneas jurisprudenciales de los correspondientes tribunales y a la constitución.

En adelante esta ley estará abreviada como como **S**, y a las circunstancias del caso en concreto que se abrevian con **C**; por lo que cuando estemos analizando la "ley epistémica de la ponderación" del "principio no satisfecho" se abreviará de la siguiente manera **SPiC**; por otro lado, cuando estemos analizando la "ley epistémica de la ponderación" del "principio contrario" se abreviará **SPjC**. (Alexy, 2019a)

6.6. Los subprincipios

Para entender a cabalidad la "fórmula del peso" es necesario ver qué circunstancias debemos analizar en cada subprincipio de *idoneidad, necesidad y proporcionalidad en sentido estricto*, aspecto que se puede apreciar del siguiente cuadro:

Subprincipio de la proporcionalidad	**Expresan y nos permiten analizar lo siguiente:**
Idoneidad y Necesidad	Los subprincipios de idoneidad y necesidad están destinados a expresar el mandato de optimización relativo a las ***posibilidades fácticas***. Lo antes dicho significa que al momento de analizar las posibilidades fácticas de la afectación de un principio y de la relevancia del otro tenemos que ponernos en un escenario en el que se trata de impedir que ocurran las referidas intervenciones, hacer que sean evitables sin generar un costo a los principios. Esto quiere decir que con los subprincipios de idoneidad y necesidad lo que buscamos es el "Óptimo de Pareto".
Proporcionalidad en sentido estricto	Este subprincipio se refiere a la optimización de los principios, pero desde las ***posibilidades jurídicas***.

Como ya lo mencionamos anteriormente, para expresar las circunstancias del caso en concreto (posibilidades fácticas) para tomar la decisión de restringir o no un derecho

utilizaremos la letra **C**. Por otro lado, para expresar la intensidad de la intervención en **Pi** utilizaremos la letra **I**, en ese sentido cuando estemos analizando la intensidad de la intervención de las circunstancias en **Pi** se abreviará de la siguiente manera **IPiC**; y cuando estemos analizando la intensidad de la intervención de las circunstancias en **Pj** se abreviará de la siguiente manera **IPjC**. (Alexy, 2019a)

6.7. La escala triádica

Ahora bien, ¿Cómo es que le asignamos un valor a estos subprincipios? Para ello, Alexy propone que para dotar a la ponderación de racionalidad se debe aplicar una clasificación o catalogación con una "escala triática" o escala de tres intensidades. La "escala triática" (Alexy, 2019) permite valorar lo siguiente:

1. El grado de no satisfacción de un derecho **IPiC**,
2. La importancia de la satisfacción del otro **WPjC** y
3. El grado de intervención de un principio **GPi,jC**.
4. El grado de seguridad de la ocurrencia de la intervención o medida examinada en el caso en concreto del "principio no satisfecho" **SPiC**.
5. El grado de seguridad de la ocurrencia de la intervención o medida examinada en el caso en concreto del "principio contrario" se abreviará **SPjC**.

Esta escala nos permitirá asignar un peso a las razones que justifican la intervención o la protección a un principio y estos pesos a su vez serán aplicados en la "fórmula del peso".

Para la valorización se utilizará una serie geométrica, con exponentes, como se verifica en el siguiente cuadro:

ESCALA TRIÁDICA PARA				
Nivel o Intensidad	**Abreviación**	**Expresa una intervención:**	**Serie Geométrica**	**Valor del nivel**
Leve	**l**	**Reducido y débil**	2^0	**1**
Medio	**m**	**Media y moderada**	2^1	**2**
Grave	**s**	**Grave, elevado y fuerte**	2^2	**4**

La razón por la cual la valorización de los niveles utiliza una serie geométrica con

exponentes es que es la manera correcta de expresar que los grados de intensidad van incrementando a medida en la que la intensidad va creciendo, eso quiere decir que en la fórmula se podrá reflejar correctamente el valor de un principio que está ganando o perdiendo fuerza cuando aumenta o disminuye la intensidad de la intervención.

Ahora bien, siendo que la potenciación o valoración de los principios que están en conflicto puede efectuarse en diferentes niveles, Alexy propone a la "escala triádica doble" para que de esta manera se valoren correctamente a estos principios ampliando la gama de intensidades como se indica en el siguiente cuadro (Alexy, 2019a):

ESCALA TRIÁDICA DOBLE			
Nivel o Intensidad	**Abreviación**	**Serie Geométrica**	**Valor del nivel**
Leve leve	**lm**	2^0	**1**
Leve moderado	**ls**	2^1	**2**
Leve grave	**ml**	2^2	**4**
Moderado leve	**ml**	2^3	**8**
Moderado moderado	**mm**	2^4	**16**
Moderado grave	**ms**	2^5	**32**
Grave leve	**sl**	2^6	**64**
Grave moderado	**sm**	2^7	**128**
Grave grave	**ss**	2^8	**256**

Ahora bien, para asignar valor a **SPiC** y **SPjC** Alexy (correspondiente a la "ley epistémica de la ponderación") propone que al valorizar el grado de seguridad de la ocurrencia de la intervención o medida examinada en el caso en concreto se deben utilizar los tres grados epistémicos que se indican a continuación (Alexy, 2019a):

ESCALA TRIÁDICA PARA SPiC - SPjC				
Nivel o Intensidad	**Abreviación**	**Expresa una intervención:**	**Serie Geométrica**	**Valor del nivel**
Seguro	**g**	**Control material intensivo**	2^0	**1**
Plausible	**p**	**Control de la plausibilidad**	2^{-1}	**0.5**
No evidentemente falso	**e**	**Control de evidencia**	2^{-2}	**0.25**

El cuadro antes indicado, también podrá ser refinado mediante una escala triádica

doble.

6.8. La fórmula del peso de Alexy

Como ya hemos indicado anteriormente, al hablar de proporcionalidad estamos hablando de una dicotomía entre el derecho de defensa y el derecho de protección y para ello Alexy propone como ejemplo el caso de la Revista satírica Titanic resuelto por los tribunales alemanes. Este caso trata sobre una publicación que hace la revista en la que se refiere a un oficial de reserva parapléjico que había logrado ser llamado nuevamente a las filas del ejército militar como "tullido", y este oficial acude a los tribunales y en primera instancia el Tribunal Superior Regional de Düsseldorf condenó a la revista a pagar una indemnización de 12 mil marcos, y el Tribunal Constitucional Federal llevó a cabo una "ponderación relativa a las circunstancias del caso en concreto" entre el derecho de la libertad de expresión y el derecho al honor del oficial. Entonces Alexy indica que ante estas situaciones nos debemos preguntar lo siguiente (debemos adaptar estas preguntas al caso en concreto que estemos analizando):

a) Para determinar la intensidad de la intervención de la libertad de expresión (es decir **Pi**) debemos preguntarnos: ¿En qué intensidad interviene en la libertad de expresión (**Pi**) la prohibición del calificativo "tullido" y que relación tiene con la imposición de la indemnización? (**IPiC**)

b) Por otro lado, para determinar la importancia de la satisfacción del principio al honor (es decir **Pj**), debemos preguntarnos en sentido contrario: ¿Qué significa para el derecho al honor que se omitiese la intervención en la libertad de expresión o no fuese ejecutada, es decir, si el apelativo de "tullido" fuese catalogado como permitido y en consecuencia no se condenara al pago de una indemnización? (**WPjC**)

Estas preguntas nos ayudarán a valorar cada derecho, asignarle un peso y nos harán reflexionar sobre los costes que se requieren para la protección del derecho al honor (**Pj**). Es así como en el ejemplo propuesto la importancia del principio de protección al honor (**Pj**) en el caso Titanic resulta del cálculo acerca de cuán intensa sería la intervención en

el derecho al honor (**Pj**) del oficial de no llevarse a cabo una intervención en la libertad de expresión (**Pi**) de la Revista Titanic.

Ahora bien, aplicando lo explicado en el transcurso del presente capítulo a continuación presentamos a la fórmula del peso de Alexy:

$$GPi,jC = \frac{IPiC \cdot GPiA \cdot SPiC}{WPjC \cdot GPjA \cdot SPjC}$$

Esta fórmula expresa que el peso el principio **Pi** en relación con el principio **Pj** en las circunstancias del caso concreto que resulta del cociente entre el producto de la afectación del principio **Pi** en concreto, su peso abstracto y la seguridad de las premisas empíricas relativas a su afectación, y por otra parte el producto de la afectación del principio **Pj** en concreto, su peso abstracto y la seguridad de las premisas empíricas relativas a su afectación.

Desarrollando el contenido de esta fórmula tenemos lo siguiente:

IPiC	=	El grado de no satisfacción de un derecho **IPiC**
WPjC	=	La importancia de la satisfacción de **Pj**
GPiA	=	Peso Abstracto de **Pi**
GP,jA	=	Peso Abstracto de **Pj**
SPiC	=	El grado de seguridad de la ocurrencia de la intervención o medida examinada en el caso en concreto del "principio no satisfecho" **SPiC**.
SPjC	=	El grado de seguridad de la ocurrencia de la intervención o medida examinada en el caso en concreto del "principio contrario" se abreviará **SPjC**.
GPi,jC	=	Peso o grado de intervención de un principio **GPi,jC**

GPiA en **GPjA** son un nuevo elemento de la fórmula del que recién hablamos y que

trata del peso abstracto (A) de **Pi** y de **Pj** al que se denomina **GPiA** y **GPjA** respectivamente. El peso abstracto es el peso que se asigna a **Pi** y a **Pj** en relación con otros principios, independientemente de las circunstancias del caso en concreto, como por ejemplo el derecho a la vida es de mayor peso que el derecho a la libertad. Los pesos abstractos sólo juegan un papel importante en la fórmula cuando los principios en colisión se diferencian en su peso abstracto. Cuando los pesos abstractos son iguales, entonces se neutralizan mutuamente.

Un clásico ejemplo para aplicar la fórmula del peso de Alexi es la colisión de derechos que se presenta cuando los padres de una niña se niegan a llevarla al hospital a hacerle una operación y un tratamiento de transfusión de sangre pues la religión que profesan lo prohíbe, siendo que este derecho colisiona con el derecho a la vida y el derecho de salud de la niña. (Bernal Pulido, 2003, p. 226)

"Principio no satisfecho" **Pi**	**vs**	**"Principio contrario"** **Pj**
Derecho a la Vida[1]		Derecho a la libertad de religión[2]

Una vez que hemos identificado los derechos en colisión, corresponde verificar el grado de afectación de cada derecho en este caso en concreto iniciando con **Pi** (**GPi**,**jC**) y luego con **Pj** (**GPj**,**iC**) como se indican a continuación:

<u>En cuanto a GPi,jC</u>:

a) Para eso vamos a empezar con establecer el grado de afectación en el "principio no satisfecho" **Pi** y para ello debemos hacernos la siguiente pregunta:

*Para determinar la intensidad de la intervención del derecho a la vida (**Pi**)*

[1] El inciso 1 del Artículo 2 de la Constitución indica que toda persona tiene derecho a la vida. Asimismo, el Artículo 7 de la Constitución establece que todos tienen derecho a la protección de su salud, la del medio familiar y la de la comunidad, así como el deber de contribuir a su promoción y defensa. La persona incapacitada para velar por sí misma a causa de una deficiencia física o mental tiene derecho al respeto de su dignidad y a un régimen legal de protección, atención, readaptación y seguridad.

[2] El inciso 2 del Artículo 2 de la Constitución indica que toda persona tiene derecho a la libertad de conciencia y de religión, en forma individual o asociada. No hay persecución por razón de ideas o creencias. No hay delito de opinión. El ejercicio público de todas las confesiones es libre, siempre que no ofenda la moral ni altere el orden público.

*debemos preguntarnos: ¿En qué intensidad interviene en la libertad de religión (**Pi**) al impedir que una niña acceda a un tratamiento médico para salvar su vida?*

Como notamos la intensidad es muy grave (más precisamente grave grave) por lo que a **IPiC** le daremos un valor de **256**.

b) A continuación, vamos a establecer el grado de la importancia de la satisfacción de **Pj** el "Principio contrario" (**WPjC**) y para ello debemos hacernos la siguiente pregunta:

*Por otro lado, para determinar la importancia de la satisfacción del derecho a la libertad de religión (**Pj**), debemos preguntarnos en sentido contrario: ¿Qué significa para a la libertad de religión que se impida que una niña acceda a un tratamiento médico para salvar su vida, es decir, que la niña fallece como consecuencia de no acceder al tratamiento médico?*

Como notamos la intensidad en la intervención al derecho de libertad de religión no es significativa en el caso en concreto (más precisamente leve leve) por lo que a **WPjC** le daremos un valor de **1**.

c) Seguidamente veremos al peso abstracto de cada uno de los principios. Como es evidente, en este caso el derecho a la vida tiene mayor peso que el derecho a la libertad de religión por cuanto para ejercer esta libertad se necesita de vida además este criterio está ampliamente desarrollado por la jurisprudencia de los tribunales peruanos. En ese sentido asignaremos los siguientes valores:

- Para **GPiA** (derecho a la vida) = **256**
- Para **GP**,**jA** (derecho a la libertad de religión) = **4**

d) Por último, tenemos que valorar la seguridad de las apreciaciones empíricas que versan sobre la afectación de las medidas en el caso en concreto (**SPiC** y **SPjC**). Para ello analizamos el grado de seguridad de que en caso los padres decidan no llevar a la niña al hospital e impedir que los médicos apliquen los tratamientos

médicos tenga como consecuencia la muerte de la menor. En ese sentido asignaremos una intervención "Segura" (g) y los siguientes valores:

- Para **SPiC** = **1**
- Para **SPjC** = **1**

En consecuencia, tenemos que el resultado con la fórmula del peso es la que se indica a continuación:

$$\mathbf{GPi,jC} = \frac{\mathbf{IPiC} \cdot \mathbf{GPiA} \cdot \mathbf{SPiC}}{\mathbf{WPjC} \cdot \mathbf{GPjA} \cdot \mathbf{SPjC}}$$

$$\mathbf{GPi,jC} = \frac{256 \cdot 256 \cdot 1}{1 \cdot 4 \cdot 1}$$

$$\mathbf{GPi,jC} = \frac{65{,}536}{4}$$

$$\mathbf{GPi,jC} = 16{,}384$$

Como consecuencia tenemos que **Pi** tiene un peso de **16,384**.

<u>En cuanto a GPj,iC</u>:

a) Empezamos con establecer el grado de afectación en el "principio contrario" **Pj** con la siguiente pregunta:

*Para determinar la intensidad de la intervención en el derecho a la libertad de religión (**Pj**) debemos preguntarnos: ¿En qué intensidad interviene en el derecho a la vida el derecho de libertad de religión (**Pi**) al impedir que se ejerza libremente una religión impidiendo que una niña acceda a un tratamiento médico para salvar su vida?*

Como notamos la intensidad es leve (más precisamente leve grave) por lo que a **IPiC** le daremos un valor de **4**.

b) A continuación, vamos a establecer el grado de la importancia de la satisfacción de **Pi** el "Principio no satisfecho" (**WPiC**) y para ello debemos hacernos la siguiente pregunta:

¿Qué significa para el derecho a la vida que para respetar el derecho a la libertad de religión se impida a una niña acceder a un tratamiento médico para salvar su vida?

Como notamos la intensidad en la intervención es grave grave por lo que a **WPiC** le daremos un valor de **256**.

c) En cuanto al peso abstracto asignaremos los siguientes valores:

- Para **GP**,**jA** (derecho a la libertad de religión) = **4**
- Para **GPiA** (derecho a la vida) = **256**

d) Por último, tenemos que valorar la seguridad de las apreciaciones empíricas que versan sobre la afectación de las medidas en el caso en concreto (**SPiC** y **SPjC**). Para ello analizamos el grado de seguridad de que en caso los padres decidan no llevar a la niña al hospital e impedir que los médicos apliquen los tratamientos médicos tenga como consecuencia la muerte de la menor. En ese sentido asignaremos una intervención "Segura" (g) y los siguientes valores:

- Para **SPiC** = **1**
- Para **SPjC** = **1**

En consecuencia, tenemos que el resultado con la fórmula del para **GPj,iC** peso es la que se indica a continuación:

$$\mathbf{GPj,iC} = \frac{\mathbf{IPjC} \cdot \mathbf{GPjA} \cdot \mathbf{SPjC}}{\mathbf{WPiC} \cdot \mathbf{GPiA} \cdot \mathbf{SPiC}}$$

$$\mathbf{GPj,iC} = \frac{4 \cdot 4 \cdot 1}{256 \cdot 256 \cdot 1}$$

$$\mathbf{GPj,iC} = \frac{16}{65{,}536}$$

$$\mathbf{GPj,iC} = \mathbf{0.0002441406}$$

Como consecuencia tenemos que **Pj** tiene un peso de **0.0002441406**.

Conclusión: La satisfacción de la libertad de religión es de **0.0002441406** y por lo tanto no justifica que este derecho intervenga en el derecho a la vida y la salud de la niña que está afectado en **16,384**. Siendo que como resultado de esta ponderación se debe privilegiar el derecho a la vida de la vida a la menor y ordenar que los padres ingresen a la niña al hospital y permitir se le apliquen todos los tratamientos necesarios.

6.9.Aplicación de la fórmula del peso en el caso del padrón electoral

A continuación, aplicaremos la fórmula del peso para intentar resolver el caso del padrón electoral desarrollado en el punto 4.1 del Capítulo IV del presente trabajo. En el caso materia de análisis los derechos en contraposición son los siguientes:

"Principio no satisfecho" Pi		**"Principio contrario" Pj**
Derecho al acceso a la información pública	**vs**	Derecho de protección de datos personales

Al aplicar la fórmula del peso tenemos lo siguiente:

<u>En cuanto a GPi,jC</u>:

a) Empecemos con establecer el grado de afectación en el "principio no satisfecho" es decir el derecho de acceso a la información pública **Pi** y para ello debemos hacernos la siguiente pregunta:

*Para determinar la intensidad de la intervención del derecho de acceso a la información pública (**Pi**) debemos preguntarnos: ¿En qué intensidad interviene en el derecho de acceso a la información pública (**Pi**) al impedir que se remita el Padrón Electoral a las autoridades del Jurado Nacional de Elecciones para que resuelvan adecuadamente los recursos de nulidad y puedan confirmar el número de votantes y confirmar si es que existen o no errores de llenado en el Acta Electoral?*

Como notamos la intensidad es muy grave (más precisamente grave grave) por lo que a **IPiC** le daremos un valor de **256**. Esto es así pues no solo hablamos del derecho de acceso a la información pública, sino que la información que de la que estamos hablando servirá, en este caso en concreto, para conocer y validar la verdad electoral de los ciudadanos y legitimar de poder al presidente del país.

b) A continuación, vamos a establecer el grado de la importancia de la satisfacción de **Pj** el "Principio contrario", derecho de protección de datos personales (**WPjC**) y para ello debemos hacernos la siguiente pregunta:

¿Qué significa para el derecho de protección de datos personales que se impida a los jurados y demás autoridades electorales el acceso de los padrones electorales para resolver las nulidades a actas electorales en las elecciones presidenciales del país?

Como notamos la intensidad de la importancia en la intervención al derecho de protección de datos personales, en las circunstancias del caso en concreto, no es significativa en el caso en concreto (más precisamente moderado grave) por lo que a **WPjC** le daremos un valor de **32**.

c) Seguidamente veremos al peso abstracto de cada uno de los principios. Como es

evidente, en este caso en concreto asignaremos el mismo valor abstracto a estos derechos:

- Para **GPiA** (derecho al acceso a la información pública) = **64**
- Para **GPjA** (derecho de protección de datos personales) = **64**

d) Por último, tenemos que valorar la seguridad de las apreciaciones empíricas que versan sobre la afectación de las medidas en el caso en concreto (**SPiC** y **SPjC**).

Para ello analizamos el grado de seguridad de que en caso la ONPE decida no proporcionar los padrones electorales a los jurados y autoridades electorales tenga como consecuencia la deslegitimación de la proclamación del presidente del país. En ese sentido asignaremos una intervención "Plausible" (p) y los siguientes valores:

- Para **SPiC** = **0.5**
- Para **SPjC** = **0.5**

En consecuencia, tenemos que el resultado con la fórmula del peso es la que se indica a continuación:

$$\mathbf{GPi,jC} = \frac{\mathbf{IPiC} \bullet \mathbf{GPiA} \bullet \mathbf{SPiC}}{\mathbf{WPjC} \bullet \mathbf{GPjA} \bullet \mathbf{SPjC}}$$

$$\mathbf{GPi,jC} = \frac{256 \bullet \cancel{64} \bullet 0.5}{32 \bullet \cancel{64} \bullet 0.5}$$

Como sabemos, cuando los pesos abstractos que tienen el mismo valor se neutralizan mutuamente.

$$\mathbf{GPi,jC} = \frac{128}{16}$$

$$\mathbf{GPi,jC} = 8$$

Como consecuencia tenemos que **Pi** tiene un peso de **8**.

<u>En cuanto a GPj,iC</u>:

a) Empezamos con establecer el grado de afectación en el "principio contrario" derecho de protección de datos personales **Pj** con la siguiente pregunta:

¿Qué significa para el derecho de protección de datos personales que la ONPE remita los padrones electorales a los jurados y autoridades electorales y no se limitara su acceso?

Como notamos la intensidad es moderado (más precisamente moderado grave) por lo que a **IPiC** le daremos un valor de **32**.

b) Para grado de la importancia de la satisfacción de **Pi** el "Principio no satisfecho" (**WPiC**) y para ello debemos hacernos la siguiente pregunta:

¿Qué significa para el derecho al acceso a la información pública que se prohíba que la ONPE remita los padrones electorales a los jurados y autoridades electorales y no se limitara su acceso?

Como notamos la intensidad en la intervención al grave grave por lo que a **WPiC** le daremos un valor de **256**.

c) En cuanto al peso abstracto asignaremos los siguientes valores:

- Para **GPjA** (derecho de protección de datos personales) = **64**
- Para **GPiA** (derecho al acceso a la información pública) = **64**

d) Para valorar la seguridad de las apreciaciones empíricas que versan sobre la afectación de las medidas en el caso en concreto (**SPiC** y **SPjC**) los siguientes valores:

- Para **SPiC** = **0.5**

– Para **SPjC** = **0.5**

En consecuencia, tenemos que el resultado con la fórmula del para **GPj,iC** peso es la que se indica a continuación:

$$\mathbf{GPj,iC} = \frac{\mathbf{IPjC} \bullet \mathbf{GPjA} \bullet \mathbf{SPjC}}{\mathbf{WPiC} \bullet \mathbf{GPiA} \bullet \mathbf{SPiC}}$$

$$\mathbf{GPj,iC} = \frac{32 \bullet \cancel{64} \bullet 0.5}{256 \bullet \cancel{64} \bullet 0.5}$$

Como sabemos, cuando los pesos abstractos que tienen el mismo valor se neutralizan mutuamente.

$$\mathbf{GPj,iC} = \frac{16}{128}$$

$$\mathbf{GPj,iC} = 0.125$$

Como consecuencia tenemos que **Pj** tiene un peso de **0.125**.

Conclusión: La satisfacción del derecho de protección de datos personales es de **0.125** y por lo tanto no justifica que este derecho intervenga en el derecho al acceso de información pública que está afectado en **8**. Siendo que como resultado de esta ponderación se debe privilegiar el derecho al acceso de información pública y ordenarse que se remitan los padrones electorales a los jurados y autoridades electorales con la finalidad de que puedan resolver los recursos de nulidad sobre las actas electorales y emitir un pronunciamiento que legitime al presidente electo del país respetando la voluntad popular. Evidentemente, la información personal contenida en el padrón electoral deberá pasar por un proceso previo de disociación de la información personal protegida y hacer una versión pública del documento.

6.10. Consideraciones adicionales sobre el conflicto entre el derecho de acceso a la

información pública y el derecho de protección de datos personales

Para romper con la llamada “cultura del secreto” en el país, la autoridad que tengan que resolver este tipo de controversias debería preferir, ante todo, el principio de máxima divulgación y permitir el acceso a la información pública, así como la libertad de información y de expresión.

Asimismo, como hemos verificado existen situaciones controvertidas en las que diferentes autoridades del país muestran percepciones distintas respecto de si es que determinado documento, como el Padrón Electoral, por ejemplo, puede ser publicado conforme al derecho de acceso a transparencia o si es que se debe evitar su publicación por respeto al derecho de protección de datos personales. Este tipo de situaciones reduce la predictibilidad y aumenta la desconfianza de los ciudadanos en el funcionamiento de las entidades públicas.

Hemos explicado, también, que la Autoridad Nacional de Transparencia y Acceso a la Información Pública, el Tribunal de Transparencia y Acceso a la Información Pública y la Autoridad Nacional de Protección de Datos Personales son los tres órganos y actores principales que dirimen las controversias referidas a protección de datos personales y acceso a la información, y hemos detallado que, a pesar de hallarse adscritos al Ministerio de Justicia y Derechos Humanos, operan con dinámicas diferentes y discrepan en cuanto a los criterios que aplican a diversos casos.

El modelo en cuestión es rechazado por los expertos internacionales en la materia; de hecho, su recomendación es que se cree un órgano mixto con autonomía jurídica que garantice la correcta aplicación de estos derechos constitucionales y genere predictibilidad y seguridad jurídica. Al respecto, también advertimos del bajo nivel de cumplimiento de remisión de informes por parte de las entidades públicas ante la Autoridad, que los requiere para elaborar el Informe Anual. Dado que la Autoridad tiene escasa capacidad para sancionar a funcionarios y tampoco cuenta con presupuesto para capacitación más efectiva, resulta muy difícil que alcance sus objetivos. A la fecha, buena parte de los funcionarios públicos vienen adaptándose todavía a las nuevas herramientas digitales para el envío de la información. (Autoridad Nacional de Transparencia y Acceso a la Información Pública, 2022, p. 123)

Los países que han desarrollado los mejores modelos para este tipo de órganos son México, Uruguay y Argentina. México tiene al Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales de México – INAI, que es un organismo público autónomo y especializado encargado de facilitar y garantizar, a la vez, tanto el acceso de las personas a la información pública como el acceso y protección de los datos personales; por lo tanto, promueve la cultura de la transparencia en la gestión pública y la rendición de cuentas del gobierno a la sociedad. Es de destacar que la norma de transparencia de México prevé que, ante la omisión de la respuesta a una solicitud de información, se aplica el silencio administrativo positivo, por lo que, en estos casos, el sujeto obligado tiene que entregar la información requerida de todas formas. Asimismo, en México se exige que los sujetos obligados a proporcionar información de carácter público desarrollen índices públicos con la información que se considera reservada. (Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales de México – INAI, 2020)

Por último, y ante la necesidad de crear una Autoridad Mixta, a fin de procurar un verdadero equilibrio entre los derechos de protección de datos personales, derecho de acceso a la información pública, derecho de libertad de expresión y de información, es que la misma Autoridad ha impulsado el Proyecto de Ley Nro. 07870/2020-PE para promulgar la Ley que crea a una autoridad mixta denominada "Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales". Éste sería un organismo técnico especializado adscrito al Ministerio de Justicia y Derechos Humanos, con autonomía técnica, funcional, administrativa, económica y financiera con representación jurídica propia.

Este Proyecto de Ley plantea, además, un régimen sancionador para los funcionarios públicos que incumplan con las obligaciones de proporcionar la información pública que se les solicita.

Si bien este proyecto de ley se encuentra actualmente archivado en el Congreso de la República, consideramos que constituye un buen punto de partida para trabajar en aras del equilibrio de cuidado de derechos varias veces referido. Es la misma Autoridad la que

se hace autocrítica y ve la necesidad de crear este nuevo organismo, que aplique de manera proporcional los derechos materia de análisis. (Ministerio de Justicia y Derechos Humanos, 2020)

CONCLUSIONES

1) El grado de flexibilidad o de rigidez en la regulación para recopilar y tratar datos, tanto por parte del propio Estado como por parte de entidades privadas, dependerá de los antecedentes históricos y necesidades propias de cada país. Vemos que, en el caso de Europa, debido a los terribles acontecimientos de la Segunda Guerra Mundial, surgió una gran necesidad de imponer estándares altos para la protección de la privacidad y de los datos personales de sus ciudadanos. Por su parte, en Estados Unidos, este derecho es reconocido a través de la jurisprudencia de los tribunales de justicia y es aplicado primordialmente en materia de derechos del consumidor, privilegiando la transparencia y derechos a la libertad de expresión y de información.

   Perú, desde hace muchos años, padece de graves problemas de corrupción, en buena medida debido a que cunde una "cultura de secreto". A pesar de ello, la legislación peruana ha adoptado en gran medida el modelo de la legislación europea. En muchos casos prefiere la privacidad y la protección de los datos personales, cuando en realidad debería primar el acceso a la información pública y el derecho a la libertad de expresión y de información para combatir de manera real a la corrupción, sobre todo tomando en cuenta los antecedentes de manipulación de data aquí registrados.

2) Se ha podido verificar que las resoluciones que la Autoridad Nacional de Transparencia y Acceso a la Información Pública (ANTAIP) emitió desde que inició sus funciones en 2017, como órgano de segunda instancia respecto de las apelaciones que efectuaron los funcionarios públicos que, en primera instancia, han recibido una sanción por haber incumplido la Ley de Transparencia y Acceso a la Información Pública, han sido declaradas unas improcedentes, otras nulas o, finalmente, fundadas. Improcedentes porque el apelante ha sido el denunciante, y no siendo parte del procedimiento administrativo disciplinario carece de legitimidad para presentar recurso de apelación. Nulos o fundados los recursos de apelación del funcionario público, porque la ANTAIP constató que el procedimiento administrativo sancionador disciplinario ha tenido actos que no se ajustan al debido proceso; por ejemplo, debido a fallas en la notificación de funcionarios, errores en la tipificación de la conducta sancionable administrativamente conforme a lo establecido en una norma con rango

de ley, o debido a que la entidad no recabó la información relevante para verificar si es que el funcionario había cometido o no falta grave; asimismo, a que no se motivó correctamente una decisión.

Todo ello evidencia que aún queda un largo camino por recorrer a fin de que las entidades y funcionarios públicos apliquen correctamente la Ley de Acceso a la Información Pública. Con esto se garantizaría el derecho de acceso a la información pública y la transparencia, a fin de que los ciudadanos puedan ejercer su derecho de fiscalización.

3) En el Perú, los tres órganos y actores principales que dirimen las controversias referidas a protección de datos personales y acceso a la información son: la Autoridad Nacional de Transparencia y Acceso a la Información Pública, el Tribunal de Transparencia y Acceso a la Información Pública y la Autoridad Nacional de Protección de Datos Personales. Como ha sido demostrado a lo largo del presente trabajo, estos órganos, a pesar de estar adscritos al Ministerio de Justicia y Derechos Humanos, en vez de tener las mismas directrices, funcionan con dinámicas diferentes e incluso discrepan entre ellas mismas emitiendo criterios contradictorios en perjuicio de la transparencia y limitando el derecho al acceso a la información pública.

   Por ello, en los casos en los que se tenga que resolver controversias con contraposición de derechos constitucionales, como el derecho de protección de datos personales y el derecho al acceso a la información pública o el derecho a la libertad de información y de expresión, el órgano competente deberá procurar un equilibrio en la ponderación de estos derechos, en base a criterios objetivos, analizando a detalle el tipo de información que está en controversia, y para ello, necesariamente tendrán que aplicar el test de proporcionalidad que consiste en examinar el tratamiento diferenciado entre dos derechos, aplicando para ello tres sub principios: (*i*) idoneidad, (*ii*) necesidad y (*iii*) ponderación o proporcionalidad en sentido estricto.

4) El modelo con el que cuenta Perú actualmente, implementado para resolver casos referentes al acceso a la información y datos personales, es uno rechazado por expertos internacionales. Lo ideal sería optar por un órgano mixto con autonomía jurídica que garantice la correcta aplicación de estos derechos constitucionales y genere

predictibilidad y seguridad jurídica; asimismo, que prevea sanciones para las entidades y funcionarios públicos que incumplan con lo establecido en la Ley de Transparencia y Acceso a la Información Pública.

RECOMENDACIONES

- Debe implementarse una autoridad mixta que se encargue de dirimir toda controversia derivada de la protección de datos personales y derecho de acceso a la información. Esta autoridad debe ser independiente y autónoma.

- La autoridad debe programar más y mejores capacitaciones, así como facilidades para que los funcionarios públicos puedan cumplir con proporcionar la información pública a los ciudadanos.

REFERENCIAS

Alexy, R. (2019a). La fórmula del peso. In Palestra Editores S.A.C (Ed.), *Ensayos sobre la teoría de los principios y el juicio de proporcionalidad* (Primera). Palestra Editores S.A.C.

Alexy, R. (2019b). La ponderación en la aplicación del derecho. In Palestra Editores S.A.C (Ed.), *Ensayos sobre la teoría de los principios y el juicio de proporcionalidad* (Primera). Palestra Editores S.A.C.

Autoridad Nacional de Protección de Datos Personales. (2022). *Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Balance de Gestión 2018 - 2021*.

Autoridad Nacional de Transparencia y Acceso a la Información Pública. (2022). *Informe Anual 2021 Sobre pedidos de acceso a la información a las entidades públicas*. https://www.gob.pe/institucion/minjus/informes-publicaciones/2987539-informe-anual-2021-sobre-pedidos-de-acceso-a-la-informacion-a-las-entidades-publicas

BBC Mundo. (2018). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. https://www.bbc.com/mundo/noticias-43472797

Bernal Pulido, C. (2003). Estructura y límites de la ponderación. *Doxa: Cuadernos de Filosofía Del Derecho*, *26*, 225–238. http://rua.ua.es/dspace/handle/10045/10074

Bernal Pulido, C. (2006). La racionalidad de la ponderación. *Revista Española de Derecho Constitucional*, *77*, 51–75. https://dialnet.unirioja.es/servlet/articulo?codigo=2233706

Black, E. R. (2001). *IBM y el holocausto* (Atlantida Editorial S.A, Ed.; Primera Edición).

Boyd v. United States, (1886). https://supreme.justia.com/cases/federal/us/116/616/#tab-opinion-1911017

Cabezas Poma, A. K. (2020). El derecho al olvido en el proceso de habeas data en el Perú. In L. R. Sáenz Dávalos (Ed.), *El Habeas Data en la actualidad* (Primera Edción). Tribunal Constitucional Centro de Estudios Constitucionales.

Carbonell, M. (2021, October 30). *Master class: Ponderación y proporcionalidad*. YouTube. https://www.youtube.com/watch?v=mzuXnZhvbr8

Cavanagh, G., & Hernández, A. (2016, October 11). *Generación perdida: los niños robados durante la dictadura argentina descubren su verdadera identidad*. Vice. https://www.vice.com/es/article/pa9dp9/generacion-perdida-argentina-orgullo-heridas-identidad

Congreso de la República del Perú. (2002). *Debate del texto sustitutorio contenido en el dictamen de la Comisión de Constitución, Reglamento y Acusaciones Constitucionales, por el que se propone la Ley de Transparencia y Acceso a la Información Pública*.

Defensoría del Pueblo. (2001). *El Acceso a la Información Pública y la Cultura del Secreto*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.defensoria.gob.pe/wp-content/uploads/2018/05/informe_60.pdf

Defensoría del Pueblo. (2022, February 17). *Nota de Prensa n.° 097/OCII/DP/2022 Defensoría del Pueblo: se registran más de 27 000 casos de corrupción en trámite en todo el país*.

https://www.gob.pe/institucion/defensoria/noticias/584422-defensoria-del-pueblo-se-registran-mas-de-27-000-casos-de-corrupcion-en-tramite-en-todo-el-pais

Dirección de Transparencia y Acceso a la Información Pública y Portección de Datos Personales. (2018). *Informe Jurídico N° 002-2018-JUS/DGTAIPD.*

Espinosa-Saldaña Barrera Eloy. (2018). *Informe sobre el principio o test de proporcionalidad en la jurisprudencia del Tribunal Constitucional peruano* . chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.venice.coe.int/webforms/documents/?pdf=CDL-JU(2019)008-spa

Frank Walker. (2017, July 30). *'Traitors' book extract: IBM's secret Nazi past*. https://www.news.com.au/finance/business/technology/traitors-book-extract-ibms-secret-nazi-past/news-story/3bde86cdeeefa44c55b90c5d568cc545

Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales de México – INAI. (2020, May 12). *Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales de México – INAI.*

Kershner, M. (2021, July 15). *Data is the new oil*. Forbes. https://www.forbes.com/sites/theyec/2021/07/15/data-isnt-the-new-oil--time-is/?sh=1d5b365035bb

Ministerio de Justicia y Derechos Humanos. (2020). *Proyecto de Ley Nro. 07870/2020-PE.* https://www2.congreso.gob.pe/sicr/tradocestproc/Expvirt_2011.nsf/visbusqptramdoc1621/07870?opendocument

Ministerio de Relaciones Exteriores, C. I. y C. de A. (2017). *Ayúdanos a encontrarte Campaña Internacional por el Derecho a la Identidad*. Ministerio de Relaciones Exteriores, Comercio Internacional y Culto de Argentina.

Molina Theissen, A. L. (1988). La desaparición forzada de personas en America Latina. *Corte Interamericana de Derechos Humanos*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.corteidh.or.cr/tablas/a12028.pdf

Morales Campos, A. (2018). Casa Londres 38: centro de tortura y sitio de memoria en Chile. *Revista Culturales*, *6*(e336). https://www.scielo.org.mx/pdf/cultural/v6/2448-539X-cultural-6-e336.pdf

Nieves Saldaña, M. (2011). El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego. *Revista de Teoría y Realidad Constitucional* , *28*, 280–283. http://e-spacio.uned.es/fez37/public/view/bibliuned:TeoriayRealidadConstitucional-2011-28-2070

Nieves Saldaña, M. (2012). «The right to privacy»: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis. *Revista De Derecho Político*, *85*, 207–213. https://revistas.uned.es/index.php/derechopolitico/article/view/10723

Olmstead v. United States, (1928). https://supreme.justia.com/cases/federal/us/277/438/

Opinión Consultiva N° 037-2019-JUS/DGTAIPD, (June 26, 2019).

Opinión Consultiva Nro. 025-2021-JUS/DGTAIPD, (July 28, 2021). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cdn.www.gob.pe/uploads/document/file/2046091/Sobre%20publicidad%20de%20datos%20personales%20contenidos%20en%20el%20Padr%C3%B3n%20Electoral.pdf

Opinión Consultiva Nro. 036-2021-JUS/DGTAIPD, (September 16, 2021).

Proética. (2021). *PROETICA*. http://dashboard.proetica.org.pe/Webdash1.aspx

Raydan, C. (2013). Origen y expansión mundial de la fotografía. *Perspectivas. Revista de Historia, Geografía, Arte y Cultura*, 133–135. http://perspectivas.unermb.web.ve/index.php/Perspectivas/issue/view/18/N%C3%BAmero%20Completo

Resolución Nº 0636-2021-JNE, (June 16, 2021). https://busquedas.elperuano.pe/normaslegales/confirman-la-resolucion-n-03283-2021-jee-lic2jne-emitida-resolucion-n-0636-2021-jne-1967192-1/

Resolución Directoral Nro. 045-2015-JUS/DGPDP, (December 30, 2015).

Roseth, B. R. A. F. P. P. M. V. H. A. S. P. N. E. E. L. L. S. F. P. (2018). *El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital* (B. R. A. S. C. Roseth, Ed.). Banco Interamericano de Desarrollo. http://dx.doi.org/10.18235/0001150

Russell, S., & Norving, P. (2015). *Artificial Intelligence: a modern approach* (Pertince Hall).

Santillán Vásquez, M. (2018). La etapa de evolución social en la que nos encontramos ya está fusionada con la inteligencia artificial, mucho más allá de cualquier punto de retorno. *Contexto*, *29*. https://www.redalyc.org/articulo.oa?id=570660792012

Sentencia Exp. 21-2001, (July 3, 2003).

Sentencia Exp. 011-2001, (August 8, 2001).

Sentencia Exp. 2235-2004-AA/TC, (February 18, 2005). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.tc.gob.pe/jurisprudencia/2005/02235-2004-AA.pdf

Sentencia TC Exp. Nº 01797-2002-HD/TC, (January 29, 2003). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tc.gob.pe/jurisprudencia/2003/01797-2002-HD.pdf

Sentencia TC Exp. N° 2579-2003-HD/TC, (April 6, 2004).

Sentencia del Tribunal de Justicia de 13 de mayo de 2014, (May 13, 2014).

STARR, K. W. (1998). *REFERRAL FROM INDEPENDENT COUNSEL KENNETH W. STARR IN CONFORMITY WITH THE REQUIREMENTS OF TITLE 28, UNITED STATES CODE, SECTION 595(c)*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.govinfo.gov/content/pkg/CDOC-105hdoc310/pdf/CDOC-105hdoc310.pdf

Transparency International. (2021). *transparency.org*. https://www.transparency.org/en/countries/peru

University of Minnesota. (2018, November 28). *Hollerith Tabulating Card*. https://www.continuum.umn.edu/2018/11/power-of-the-punch-card/

BIBLIOGRAFÍA

Burga Coronel, A. M. (2011). El test de ponderación o proporcionalidad de los derechos fundamentales en la jurisprudencia del Tribunal Constitucional peruano. *Gaceta Constitucional*, *47*, 253–267. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/B01644A8B01411E905257D25007866F1/$FILE/Burga_Coronel.pdf

Cárdenas Gracia, J. (2014). Noción, justificación y críticas al principio de proporcionalidad. *Boletín Mexicano de Derecho Comparado*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.org.mx/pdf/bmdc/v47n139/v47n139a3.pdf

Clérico, L. (2018). *Derechos y proporcionalidad: violaciones por acción, por insuficiencia y por regresión Miradas locales, interamericanas y comparadas* (Instituto de Estudios Constitucionales del Estado de Querétaro Poder Ejecutivo del Estado de Querétaro, Ed.; Primera Edición). Instituto de Estudios Constitucionales del Estado de Querétaro Poder Ejecutivo del Estado de Querétaro. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.corteidh.or.cr/tablas/r38165.pdf

Covarrubias Cuevas, I. (2014). ¿Emplea el Tribunal Constitucional el test de proporcionalidad? (128 sentencias del Tribunal Constitucional en la perspectiva de la jurisprudencia constitucional alemana, de la Cámara de los Lores y del Tribunal Europeo de Derechos Humanos). *Estudios Constitucionales*, *12*(1), 163–237. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://scielo.conicyt.cl/pdf/estconst/v12n1/art05.pdf

Cuello Quiñonez, M. M., & Sardoth Redondo, A. K. (2018). *Principio de proporcionalidad y test de ponderación como técnica para dar solución a derechos fundamentales en conflicto en derecho administrativo en el tiempo posmoderno* [Universidad Santo Tomás]. https://repository.usta.edu.co/handle/11634/10756

Indecopi – Gerencia de Estudios Económicos. (2020). *Propuesta metodológica para el cálculo de multas en el Indecopi* (Indecopi – Gerencia de Estudios Económicos, Ed.). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.indecopi.gob.pe/documents/1902049/4214623/DT+Multas+18052020.pdf/0259ddcd-ba8a-ee3a-e3cd-4e41f83a4e7b

Mariscal Rivera, M. P. (2019). Aplicación del test proporcionalidad en la argumentación de las resoluciones judiciales en el ámbito del derecho civil. *Revista de Derecho: Universidad Nacional Del Altiplano de Puno*, *2*, 153–174. https://dialnet.unirioja.es/servlet/articulo?codigo=7605953

Orozco Solano, V. E. (2013). La ponderación como técnica de aplicación de las normas sobre derechos fundamentales: una sentencia emitida por el tribunal constitucional español en materia de libertad religiosa. *Revista Judicial*, *109*, 24–41. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.corteidh.or.cr/tablas/r31074.pdf

Ortiz Agudelo, M. O. (2018). La proporcionalidad como método interpretativo de la justicia transicional. *Revista de La Facultad de Derecho y Ciencias Políticas Universidad Pontificia Bolivariana*, *48*. https://doi.org/10.18566/rfdcp.v48n129.a09

Osiptel. (2023). *Metodología para la determinación de multas por infracciones a la libre y leal competencia* (Osiptel, Ed.). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.osiptel.gob.pe/media/5yyfurw5/resol025-2023-cd-informe-metodologico.pdf

Rainer, A., Martínez Estay, J. I., & Zúñiga Urbina, F. (2012). El principio de proporcionalidad en la jurisprudencia del tribunal constitucional. *Estudios Constitucionales*, *1*, 65–116. http://www.estudiosconstitucionales.cl/index.php/econstitucionales/article/view/105/95

Sotomayor Trelles, J. E. (2017). *Análisis económico del test de ponderación*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.up.edu.pe/UP_Landing/alacde2017/papers/37-Analisis-economico-test-ponderacion.pdf

Sentencia Exp. 045-2004-PI/TC, (2004). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.tc.gob.pe/jurisprudencia/2006/00045-2004-AI.pdf

Sentencia Tribunal Constitucional EXP.N. 579-2008-PA/TC, (2008). https://www.tc.gob.pe/jurisprudencia/2009/00579-2008-AA.html

EN BÚSQUEDA DEL EQUILIBRIO ENTRE LA PROTECCIÓN DE DATOS PERSONALES, EL DEBER DE TRANSPARENCIA Y EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

INFORME DE ORIGINALIDAD

14%	16%	8%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	www.informatica-juridica.com Fuente de Internet	2%
3	documentop.com Fuente de Internet	2%
4	bdigital.uexternado.edu.co Fuente de Internet	1%
5	idoc.pub Fuente de Internet	1%
6	qdoc.tips Fuente de Internet	1%
7	www.derechopenalenlared.com Fuente de Internet	1%
8	datospdf.com Fuente de Internet	1%