Universidad de Lima
Facultad de Derecho
Carrera de Derecho

LA INCORPORACIÓN DEL DERECHO A LA PORTABILIDAD DE DATOS PERSONALES EN EL ORDENAMIENTO JURÍDICO PERUANO

Tesis para optar el Título Profesional de Abogado

Gabriela Guadalupe Bolaños Vainstein
Código 20142406

Asesor
Carlos Raúl Jiménez Rodríguez

Lima – Perú
Marzo de 2022

INCORPORATION OF THE PERSONAL DATA PORTABILITY RIGHT WITHIN THE PERUVIAN LEGAL FRAMEWORK

TABLA DE CONTENIDO

RESUMEN

La presente investigación busca determinar, mediante una metodología dogmática y funcional si, a la luz de la legislación actual, el titular de los datos personales cuenta con adecuadas vías técnicas para reutilizar sus datos personales en el entorno digital, al ser esta una de las facultades constitucionales del derecho a la protección de los datos personales. De ser la respuesta positiva, se intentará definir qué vías y mecanismos existentes resultan adecuados ante la realidad práctica del ecosistema digital. De ser negativa, se pretenderá proponer una fórmula legal, así como consideraciones regulatorias y orientativas para abordar tal ausencia normativa.

Por ello, primero se estudiará qué son los datos, qué implica un dato de carácter personal, así como qué tipos y/o clasificaciones de datos personales existen. También, se ahondará en el contenido del régimen constitucional, legal y regulatorio previsto para la protección de datos personales, contrastando su aplicabilidad en el entorno digital y la facultad de reutilización respecto a la posibilidad de que el titular de los datos personales pueda portar sus datos personales.

Segundo, se analizarán las implicancias económicas, estudiando las particularidades del sector digital y el mercado de datos, así como la relación entre el derecho a la libre competencia en torno al acceso, trasferencia y reutilización de datos; con ello, se determinará cuáles serían las consecuencias económicas de introducir dicho derecho. Además, se estudiará qué implica la portabilidad y qué condiciones técnicas resultan necesarias para aplicarla a los datos personales.

Finalmente, se propondrán los mecanismos legales, regulatorios y orientativos idóneos para suplir tal ausencia normativa y garantizar la facultad de reutilización del titular de los datos personales en el entorno digital, en consonancia con los principios, límites y mecanismos existentes en el régimen de protección de datos personales vigentes.

Palabras clave: derecho a la portabilidad, reutilización de datos personales, Ley de Protección de Datos Personales, tratamiento automatizado de datos personales, autodeterminación informativa.

ABSTRACT

This research seeks to determine, through a dogmatic and functional methodology, if, in light of current legislation, the personal data subject has adequate technical means to reuse his personal data within the digital environment, being it a power of the personal data constitutional protection. If the answer is positive, an attempt will be made to define which existing ways and mechanisms are appropriate considering the digital ecosystem' practical reality. If negative, a legal formula will be proposed, as well as regulatory and guidance considerations to jointly address such regulatory absence.

Therefore, first the data meaning will be studied, including what implies personal data, what types and/or classifications of personal data exist. As well as delving into the content of the personal data protection constitutional, legal and regulatory regime; contrasting its applicability in the digital environment, and its reuse faculty, i.e., the possibility of the personal data subject to carry his data personal.

Second, in order to forecast some possible economic consequences of introducing the said right; the particularities of the digital sector and the data market, the relationship between the right to free competition on data access, transfer and reuse, will be also studied. In addition, the nature of portability and its necessary technical conditions for its appliance to personal data will be analyzed.

Finally, a proposal will be brought up for appropriate legal, regulatory and guidance mechanisms to drive such regulatory absence and to guarantee the right to reuse of the personal data subject within digital environment. The abovementioned, considering all principles, limits and mechanisms of the existing personal data protection regime.

Key words: Portability right, personal data reuse, Personal Data Protection Law, personal data automated processing, informational self-determination.

INTRODUCCIÓN

El interés por esta investigación nace gracias a un seminario de investigación realizado durante mi época de intercambio estudiantil en la Universidad de Bayreuth en Alemania. Este trató sobre la posición del responsable del tratamiento de datos personales frente a interferencias de terceros. En el transcurso del mismo, llamó mi atención el Reglamento General de Protección de Datos (RGPDP), que entró en vigencia el 25 de mayo de 2018. A diferencia de la Directiva anterior a la que reemplazó, este es de aplicación directa en todos los países miembros de la Unión Europea.

En ese contexto, pude conocer sobre la reciente implementación de dos derechos novedosos en dicha legislación: el derecho al olvido y el derecho a la portabilidad de datos personales. El primero, luego de amplias discusiones, fue finalmente incorporado en la Unión Europea; su introducción tendría efectos muy similares a los derechos de oposición y cancelación que se encuentran vigentes en la legislación peruana. Sin embargo, el derecho a la portabilidad dejaba entrever rápidamente la necesidad de considerar todo un trasfondo técnico y económico propio de los tratamientos automatizados en el entorno digital, el cual parecía exceder y reformular el contenido del existente derecho de acceso. Sin duda, mi interés por comprender las motivaciones de incorporar tan novedoso derecho fue en aumento.

Era evidente que el constante desarrollo tecnológico puede resultar disruptivo, incluso para el propio ordenamiento jurídico, siendo un reto propio del régimen de protección de datos personales mantener materialmente vigentes las facultades de control de lostitulares de los datos personales. Ante este reto que me propuse emprender, agradezco a todas las personas que contribuyeron a la presente investigación.

Con ello, es innegable que, en el entorno digital, el titular de los datos personales viene, de forma recurrente, participando en transacciones comerciales en las que, independientemente del servicio o producto contratado, sus datos personales son un activo esencial para llevarlas a acabo. En la actualidad, los datos son vistos como un *commodity* en similitud a las materias primas debido a que, junto con la infraestructura tecnológica para tratarlos, como la inteligencia artificial y el Big Data, derivan en un valor agregado que, por lo general, termina beneficiando enormemente (y principalmente) a los responsables del tratamiento.

En base a ello, parecería que ostentar el control fáctico sobre los datos es un factor clave, lo que ocurre por parte de quienes tienen la tecnología y herramientas necesarias para tratarlos. Esto, posiblemente, habría traído lo que algunos autores señalan como una "asimetría" en el mercado digital frente a otros agentes competidores, pues genera, entre otros efectos, fuertes barreras de entrada y, de cara a los consumidores -que, de forma recurrente, son titulares de los datos personales-, limitaciones para gozar de dichos beneficios derivados.

Así, es vital analizar si, a la luz de la legislación actual, el titular de los datos personales sigue contando con adecuadas vías técnicas para reutilizar sus datos personales, bajo la posibilidad de poder solicitar una "copia"; facultad constitucionalmente reconocida que resulta esencial para que el titular de los datos personales pueda desplegar distintas

transacciones económicas en el entorno digital, sin vulnerar o perder el control sobre sus datos personales.

Por ello, en el capítulo I se inicia estudiando el concepto de datos personales y demás actores involucrados, los alcances de su protección fundamental y el marco legal existente en la Ley Nº 29733, Ley de Protección de Datos Personales; su Reglamento, aprobado mediante Decreto Supremo Nº 003-2013-JUS; y, demás disposiciones aplicables. Lo anterior a fin de dilucidar si el contenido del derecho de acceso, al ser contrastado con las particularidades del entorno digital es suficiente para garantizar la "reutilización" de los datos personales en contraste con sectores tradicionales y tratamientos no automatizados.

En el capítulo II, se analizarán las particularidades del sector digital y los mercados de datos; qué implica la portabilidad y cuáles serían sus efectos económicos sobre el mercado y sobre el titular de los datos personales; la presencia del derecho a la competencia en el sector digital y su interacción en torno al acceso; el intercambio y la reutilización de los datos; los requerimientos técnicos para el funcionamiento de la portabilidad de datos personales en entornos digitales; las iniciativas privadas existentes para tal fin y experiencias en sectores digitales que sirven de guía para la implementación de la portabilidad en el sector de los datos personales.

Finalmente, en el capítulo III, en caso de determinarse una laguna técnica, se propondrán los mecanismos legales, regulatorios y orientativos idóneos para suplir tal ausencia normativa y garantizar la facultad de reutilización del titular de los datos personales en el entorno digital, en consonancia con los principios, límites y mecanismos existentes en el régimen de protección de datos personales vigentes.

CAPÍTULO I: NOCIÓN DE DATO PERSONAL Y SU REGULACIÓN EN EL PERÚ

1.1 Definición y diferencia entre datos y otros actores involucrados

Los datos son "la materia prima producida al abstraer el mundo en categorías, medidas y otras formas representativas (números, caracteres, símbolos, imágenes, sonidos, ondas electromagnéticas, bits) que constituyen los bloques de construcción para la información y el conocimiento" (Kitchin, 2014). Son un activo clave y poseen una naturaleza representativa de "cualquier información registrada por medios electrónicos o digitales y recuperable, ya sea perceptible para un humano o una máquina" (Ritter & Mayer, 2017).

En sede nacional, en el artículo 23.1° del Decreto Legislativo Nº 1412, Decreto legislativo que aprueba la Ley de Gobierno Digital, se encuentra la siguiente definición legal: "los datos son la representación dimensionada y descifrable de hechos, información o concepto, expresada en cualquier forma apropiada para su procesamiento, almacenamiento, comunicación e interpretación". Una característica importante, aparte de su representatividad, es su falta de neutralidad, en tanto "están enmarcados técnica, económica, ética, temporal, espacial y filosóficamente (…) no existen independientemente de las ideas, instrumentos, prácticas, contextos y conocimientos utilizados para generarlos, procesarlos y analizarlos" (Kitchin, 2014). De igual manera, Scassa (2018) indica lo siguiente:

> [L]os datos reflejan de manera inherente elecciones: elecciones sobre qué datos recopilar (o excluir) y qué herramientas o parámetros ser utilizado en su colección. Los datos derivados [de otros datos] reflejan las muchas opciones que se tomaron para determinar cómo se procesarían y con qué fines (p. 3).

Para diferenciar el concepto de datos de otros vinculados, será útil mencionar la pirámide del conocimiento[1], que, como Rowlings (2017) señala, es un modelo o construcción, a la fecha no libre de críticas y/o actualizaciones[2], que destina a los datos como materia prima para crear información; a su vez, esta para desarrollar conocimiento; y, finalmente, para generar sabiduría. Según Ackoff, cada uno de los tipos superiores de la jerarquía "incluye las categorías que se encuentran por debajo" (como se cita en Rowlings 2007, p. 164).

Cada capa de este modelo es un proceso de destilación (reducción, abstracción, procesamiento, organización, análisis, interpretación, aplicación) que agrega organización, significado y valor al revelar relaciones y verdades sobre el mundo (Kitchin, 2014). Por ello, sin ánimo de cuestionar o profundizar en el debate clasificatorio y conceptual de otras áreas de estudio, para fines didácticos, se replicará el diverso contenido doctrinario de estas categorías.

- Datos: Scassa (2018) señala que son esencialmente significativos y contienen alguna verdad-significado inicial, generalmente, denominados hechos. No obstante, algunos autores, como Kitchin (2014), consideran que los hechos son más bien una etapa previa o componentes básicos de los datos gracias a su gran representatividad. Así, los datos derivarían de estos.

- Información: agrega valor que ayuda a la interpretación, al ser los datos procesados, es decir, son los hechos contextualizados. Por su parte, Floridi menciona que agregan significado a los datos, por lo que, gracias a sus propiedades, han obtenido aceptación como un tipo especial de mercancía (como se cita en Kitchin, 2014).

[1] O por sus siglas en inglés, la Jerarquía DIKW (*data, information, knowledge, wisdom*) alude, progresivamente, a los conceptos de datos, información, conocimiento y sabiduría.

[2] Rowling (2007) concluye que, a pesar de que, normalmente, la información se define en términos de datos, el conocimiento en términos de información y la sabiduría en términos de conocimiento; hay desacuerdos en la descripción y definición de los procesos que transforman elementos inferioresen cada jerarquía superior.

Purtova (2018) menciona que, si bien el derecho se caracteriza generalmente por una mala conceptualización de la información, varios análisis han adoptado una Definición General de Información (GDI)[3] como estándar operativo: la información es la suma de los datos más su significado. Los datos representan la falta de uniformidad en el mundo; una descripción de algo que permite que se registre, analice y reorganice; y, para percibirlos como información, se les tiene que dar sentido.

Pese a que esta definición fue ampliamente adoptada, otros rechazan la idea de que la información siempre es significativa para quienes la usan. Como explica Hildebrant (2018), el significado es una función del curioso entrelazamiento de la autorreflexión, el discurso racional y la conciencia emocional, que es (todavía) una prerrogativa humana y no puede ser un elemento definitorio de información que procesan los no humanos (animales y máquinas).

La diferencia entre ambas tendencias está en considerar si solo los humanos procesan información o si se encuentra en todas partes del universo, independiente de si cualquier forma de inteligencia puede percibirlo o no. Todo puede ser una fuente de datos, pero para ser información, ¿todos los datos tienen significado? Esto depende del destinatario. Como explica Burgin, la misma información puede tener varios significados o ninguno, dependiendo de quien lo perciba (como se cita en Purtova, 2018).

Purtova (2018) recalca que, la forma en que las máquinas modernas adjuntan el significado a los datos, está más allá del alcance de la mente humana. Los nuevos algoritmos de Inteligencia Artificial (IA) funcionan como una caja negra[4], más allá de la cognición humana. Los datos almacenados en bases de datos

[3] Acrónimo del término en inglés que alude a *General Definition of Information*.

[4] Término traducido del inglés *black box* que, como Ursic (2018) señala, alude a las prácticas oscurasde procesamiento de datos que vulneran los derechos fundamentales de las personas. El autor menciona la empresa Acxiom (https://www.acxiom.com/), dedicada al mercado de datos en línea. Esta ha tenido un papel esencial en la elaboración de perfiles de los pasajeros para detectar riesgos de seguridad; sin embargo, un ciudadano nunca podría comprender cómo se determinó exactamentesu puntuación de seguridad ni el proxy usado. Como esta arquitectura de elección no es transparente

o transmitidos en vivo forman la esencia de *Big Data*[5] y tienen la capacidad de aprovechar la información de forma fundamentalmente novedosa; por ello, es más seguro asumir que todos los datos tienen un significado potencial, aunque no sea para humanos. Por tanto, según Purtova (2018), todo es dato y todos los datos tienen significado; en consecuencia, todo es o contiene información.

- Conocimiento: se obtiene "a través del procesamiento, la gestión y el uso de la información que la convierte a esta en un conocimiento [que es] aún más valioso" (Kitchin, 2018, p. 40). Weinberger señala que es el "saber hacer [*know-how*] que transforma la información en instrucciones" (como se cita en Kitchin, 2014). En este marco, el mismo autor dice que "la información son datos estructurados y el conocimiento es información procesable" (como se cita en Kitchin, 2014). Por otro lado, "para otros, es más que un conjunto de instrucciones; (…) [se refiere a] aplicar procesos cognitivos complejos como la percepción, síntesis, extracción, asociación, razonamiento y comunicación a la información (…) que se pueden utilizar para formular políticas y acciones" (Kitchin, 2014).

  Por ejemplo, según Floridi, la información semántica se puede vincular con recetas (primero haga esto, luego haga aquello, etc.) o una forma condicional de procedimientos inferenciales (si tal o cual es el caso, haga esto; de lo contrario, haga esto) (como se cita en Ritchin, 2014, p. 40).

---

ni fácil de monitorear, la autonomía y el control sobre un individuo afectado se ven inevitablemente desafiados. Por ello, el creciente procesamiento de datos personales podría diluir los derechos de las personas, siendo necesaria la protección desde nuevas perspectivas (Purtova, 2018). Para más información sobre el problema del *black box* y sesgos algorítmicos visitar el siguiente enlace: http://artificialintelligencemania.com/2019/01/10/the-black-box-problem/

5 *Big data* o los elevados volúmenes de datos reconocidos con el acrónimo de las cuatro "uves" por su volumen; variedad, tanto de tipos como de fuentes de datos; velocidad, en su captura y procesamiento; y, veracidad, con relación a su calidad. Con el tiempo, ha empezado a añadirse algunas "uves" más, como valor, variabilidad y visualización" (López, 2019). Esto ha permito, principalmente, a las grandes empresas mejorar y desarrollar nuevas operaciones internas y externas que, a su vez, dependen de una continua generación y análisis de más datos para alcanzar nuevos estándares de desarrollo.

Además, se debe resaltar que, algunos autores, identifican que la manera en la que algunos han diferenciado a los datos de la información es vía una diferenciación entre la forma (generalmente, digital), en la que se incorpora la información y el significado que contiene esa forma (la información misma): una distinción entre el nivel sintáctico de información (la forma) y el nivel semántico de información (el significado). No obstante, como Janeček (2018) aclara, este enfoque no puede brindar el nivel deseado de claridad porque confunde información sintáctica con datos. Así, se confunde el nivel sintáctico de información, como la representación formal de la información.

- Sabiduría: está en la cúspide. Según Kitchin (2014), es poder aplicar sabiamente el conocimiento (p. 40). Para ISKO Encyclopedia of Knowledge (2018), si el conocimiento era saber hacer y saber controlar los sistemas, entonces, la sabiduría era, simplemente, una cuestión de usar ese conocimiento práctico para lograr fines apropiados. Jasha (como se cita en Rowling, 2007) resalta el componente ético de este elemento, al decir que la sabiduría es la capacidad de actuar de manera crítica o práctica en cualquier situación dada. Así, se basa en un juicio ético relacionado al sistema de creencias de un individuo. Es de precisar que este elemento no ha sido muy debatido en el medio. Varios autores como Rowlings (2007) y Kitchin (2014) advierten una atención limitada a las discusiones sobre la naturaleza de la sabiduría y su desarrollo en los sistemas de información y la gestión del conocimiento.

Por su parte, el Centre on Regulation in Europe [CERRE] considera que los datos en sí no tienen ningún valor económico, ya que son simplemente la representación (digital) de señales que se han recibido o percibido utilizando alguna sintaxis. Estos se transformarán en información solo si se combinan con la semántica, es decir, si se les da un significado (en este caso, un mensaje que se comunica). De esta manera, se convertiría en información. A su vez, se pueden transformar en conocimiento procesable con la entrada adicional y/o combinación con otras piezas de información. Por ejemplo, se encuentran los *clics* (datos) en

un sitio de comercio electrónico que representan qué productos consideró un comprador para comprar (información). Luego, estos pueden usarse para inferir en qué productos podría estar interesado el mencionado comprador (conocimiento).

Lo interesante es que CERRE (2020) concluye que solo el conocimiento procesable que se genera, a partir de los datos, tiene potencialmente valor económico y puede aumentar el bienestar. Sin embargo, advierte que en la práctica comercial es habitual referirse a los tres conceptos (datos, información y conocimiento), solo como datos. En cambio, los datos brutos (conocido como *raw data* o datos sin procesar) sí suelen diferenciarse de los otros conceptos, al indicar que los otros serían datos derivados o inferidos de los primeros datos brutos. Estas diferencias serán estudiadas en el siguiente capítulo.

Se debe mencionar que las distinciones anteriores, también, tienen implicancias en el ordenamiento jurídico. A modo demostrativo más no limitativo, se presentan casos en los que se abordan reglamentaciones y/o límites de permisibilidad a ciertas actividades que implican el uso de datos, información y demás conceptos asociados a esta pirámide del conocimiento:

- En la propiedad intelectual, por ejemplo, Scassa (2018), indica que, cuando un reportero recopila hechos y los contextualiza, los constituye en información vía un artículo periodístico[6]. Consecuentemente, la ley protegerá su artículo como obra literaria (literal m del artículo 5º del Decreto Legislativo Nº 822, Ley sobre Derechos de Autor); no obstante, los simples hechos o datos[7] que relata el artículo no se tornan susceptibles de protección, sino que permanecen en dominio público, libres de tomar y reutilizarse siempre y cuando no se reproduzca la expresión original.

[6] Protegido, expresamente, en el literal m del artículo 5º del Decreto Legislativo Nº 822, Ley sobre Derechos de Autor (1996).

[7] Numeral 4 del artículo 2º del Decreto Legislativo Nº 822, Ley sobre Derechos de Autor (1996).

- En el caso del secreto empresarial en la propiedad industrial[8] (o secreto industrial), se enfatiza lo siguiente:

> [E]s toda información o conocimiento reservado o confidencial (no divulgada) que posee valor comercial para una empresa (persona o institución). El valor comercial implica que dicha información pueda ser susceptible de uso y aprovechamiento, o para obtener ventaja competitiva, en el contexto de alguna actividad productiva, industrial o comercial (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [INDECOPI], 2020, p. 6).

Los requisitos para su registro son los siguientes: ser secreta, poseer valor comercial y tener medidas razonables de protección. Asimismo, la información o conocimiento que puede ser protegida por esta figura es aquella referente a la naturaleza, características o finalidad de los productos; métodos o procesos de producción; y, medios o formas de distribución, comercialización de productos o prestación de servicios.

Desde el modelo analizado, la protección está orientada a preservar dicha información o conocimiento (quizás hasta sabiduría), que tiene valor comercial y otorga una ventaja competitiva dentro de un sector del mercado, independientemente de la materia a la que se refiera. De lo anterior, se deduce que los simples datos, vistos desde el punto de la clasificación anterior, no serían suficientes para su calificación, pues carecerían de ese valor agregado que se va obteniendo en las instancias superiores del modelo o pirámide del conocimiento[9].

- En el caso de la protección otorgada a los datos personales, la Ley Nº 29733, Ley de Protección de Datos Personales [LPDP], en el numeral 4 del artículo 2º, junto con el Reglamento de Protección de Datos Personales, aprobado

[8] Reconocido y regulado por la Decisión Nº 486, Régimen Común sobre Propiedad Industrial, y el Decreto Legislativo Nº 1044, Ley de Represión de la Competencia Desleal (2008).

[9] Ello tomando siempre en cuenta que, una instancia superior, implica a las inferiores.

mediante Decreto Supremo Nº 003-2013-JUS [Reglamento], recoge una definición expresa de dato personal: "toda información [numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo] sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados".

Al respecto, cabe adelantar que la forma en que el ordenamiento jurídico otorga esta protección es mediante un criterio que se aplica a la inversa. Así, como Janeček (2018) señala, tal criterio se encuentra tanto en la legislación de la Unión Europea[10] como en la peruana, al definirse a los datos personales como la fuente de información que, si es personal, implicará a la inversa que tales datos también sean personales. Bajo esta perspectiva, los datos no siempre son necesariamente personales desde su recopilación, pero podrán volverse en cualquier momento o circunstancia de su tratamiento, si llegan a generar información personal. Esta idea será estudiada en la siguiente sección.

1.2 Datos personales en estricto

La Organización para la Cooperación y el Desarrollo Económicos [OCDE] (2019), en recurridos documentos señala "personal data means any information relating to an identified or identifiable individual (data subject)" [dato personal significa cualquier información relacionada con un individuo identificado o identificable (titular de los datos personales)] (p. 26).

[10] La definición de la que se habla, en dicho ordenamiento jurídico, es la siguiente:

> [T]oda *información* [cursiva añadida] sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (Apartado 1 del artículo 20º del Reglamento UE 2016/679, Reglamento General de Protección de Datos Personales, 2016).

Sin embargo, la información personalmente identificable o de identificación personal (*personally identifiable information*) es definida como "any information that a) can be used to identify the PII principal [term meaining natural person to whom the personally identifiable information relates] (…), or b) is or might be directly or indirectly linked to a PII principal" [cualquier información que a) pueda usarse para identificar al principal de PII (persona física con quien se relaciona la información de identificación personal), o b) está o podría estar vinculada directa o indirectamente a un principal de PII.] (International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2017, pp. 3-4).

Como se planteó anteriormente, si bien el dato y la información son conceptos diferentes, la información implica la existencia de datos. Por ello, en el mercado no se requiere comprender previamente la información que cualquier dato pueda transmitir para que sea tratado como un activo, pues, en un futuro, dependiendo de los medios o herramientas a emplearse, se podrá extraer información valiosa. Como advierte Janeček (2018), esto conlleva a que los mismos datos puedan ser analizados indefinidamente, sobre todo, cuando son recopilados en el entorno de Internet de las Cosas (IoT)[11], lo que, a su vez, genera preocupaciones sobre la posibilidad de que puedan, eventualmente, revelar o no información personal e incluso sensible (p. 7).

[11] IoT es el acrónimo del término en inglés de Internet of Things que, como Ciani (2018) menciona, es atribuible a Kevin Ashton al haberlo, inicialmente, empleado en el título de una presentación de 1998, con el significado de "cosas que utilizan datos que recopilaron sin nuestra ayuda" (p. 216). Para el autor, los tres tipos de componentes esenciales en el IoT son los físicos (dispositivos), los de conectividad (protocolos para facilitar la comunicación entre dispositivos inteligentes) y los inteligentes: sistemas y métodos para almacenar y analizar datos. Su definición es la siguiente:

> Colección de 'dispositivos inteligentes' físicos cotidianos equipados con microchips, sensores y capacidades de comunicación inalámbrica y conectados a Internet y entre sí, que pueden recibir, recopilar y enviar una gran cantidad de datos del usuario, rastrear actividades e interactuar con otros dispositivos para brindar servicios más eficientes adaptados a las necesidades y deseos de los usuarios" (Ciani, 2018, p. 216).

Por ello, la noción de dato personal va siempre ligada a un régimen de protección legal aplicable, en tanto haya sido promulgada por el ordenamiento jurídico que, para su configuración, como en cualquier otro régimen normativo, se ponderarán distintos intereses, consideraciones y actores involucrados. Inicialmente, debe tomarse en cuenta la presencia de dos perspectivas o intereses contrarios en juego, conocidos bajo el nombre de la dicotomía o la teoría de la dualidad de los datos[12] (La Escuela de Economía y Ciencia Política de Londres, 2020), abordada por todos los ordenamientos jurídicos al configurar el marco normativo de protección de datos personales y/o información personal[13]:

- Privatista: a favor de proteger, en primera instancia, la privacidad de los individuos junto con los demás derechos fundamentales que pudiesen resultar involucrados de los individuos. Los datos deben considerarse como información que se beneficia de la protección de los derechos fundamentales.

  Al respecto, Janeček (2018) señala que dado que el control sobre cualquier dato implica también el riesgo de control sobre la información personal (no al revés), sería prácticamente imposible hacer cumplir la privacidad de la información si alguien pudiera controlar cualquier dato al poseerlo exclusivamente. Así, el autor se refiere a que considerar únicamente este razonamiento puede conducir a conclusiones radicales como eliminar el control exclusivo de datos, la propiedad de datos o, en general, cualquier tipo comercio de datos en la economía.

- Económica u orientada al mercado: como Rauhofer y Lynskey (2019) señalan, consiste en enfatizar la importancia de los datos como un producto económico, activo o insumo para bienes y servicios. Para estos autores, la

[12] "Los datos pueden considerarse tanto un activo económico como un derecho" (La Escuela de Economía y Ciencia Política de Londres, comunicación personal, agosto de 2020).

[13] A manera informativa, se aconseja visitar el siguiente enlace, el cual mide el nivel de protección delos datos personales en los ordenamientos jurídicos del mundo entero: https://www.cnil.fr/en/data-protection-around-the-world

finalidad es crear estándares comunes para la protección de datos y, así, mejorar su movimiento entre organizaciones en diferentes países, y facilitar la cooperación comercial y económica. Esta postura suele ser fuertemente defendida (o radicalizada) por los terceros que están a favor del comercio de datos y buscan extender/asegurar sus propios intereses, mediante derechos de exclusividad, obligaciones de confidencialidad, etc.[14]

A lo anterior, se debe añadir que la definición de dato personal es regulada a la inversa, pues se la define a partir del concepto de información en múltiples legislaciones. Esto es lo que Janeček (2018) denomina como el problema del huevo/gallina. Gracias a ello, el argumento privatista se enfocará en la información y sostendrá que todo dato puede revelar información personal; por otro lado, el argumento económico se centrará únicamente en los datos, acotando que estos serán únicamente personales cuando haya evidencia suficiente de que sí revelan información personal.

Siguiendo con las observaciones, la OCDE (2019), por su parte, advierte que el haberse decantado por una naturaleza binaria, entre la dicotomía de datos personales versus no personales, se generan las siguientes controversias en las definiciones legales:

- La naturaleza dinámica de los datos personales hace que los avancesactuales en el análisis de datos e IA faciliten el enlace y la relación sobre múltiples datos, aparentemente no personales, que, al unirse con otros datos (personales o no), dan como resultado información que sí resulta de carácter personal, desdibujándose fácilmente la distinción entre datos personales y no personales. Por ende, se desafía al enfoque regulatorio actual que determina la aplicabilidad de derechos, restricciones u obligaciones, mediante un concepto estático de datos personales.

[14] Un ejemplo de estos esfuerzos por proteger y dar seguridad son los anteriormente citados derechos de autor, propiedad industrial, secreto empresarial, los *sui generis database right* (aplicable y reconocido en la Unión Europea), entre varios otros para proteger los datos (muchas veces, personales), debido al valor económico que poseen en el mercado.

- Los datos personales abarcan distintos tipos de datos que, en algunos contextos, merecen ser distinguidos y tratados de manera diferente, dado el nivel de riesgos asociados con su recopilación, procesamiento y uso en cada caso[15] (p. 26).

Como solución a esta disyuntiva, Janeček (2018) propone emplear un mecanismo distinto al llamado inverso o binario, como señala la OCDE (2019a), para configurar las definiciones legales de dato personal[16]. Esta salida consistiría en identificar el componente personal en el plano de los datos y no desde el plano siguiente (de la información). Ello debido a que hay casos en los que es evidente y/o inevitable que un dato revele información personal al ser analizado, es decir, lo hará de forma intrínseca. Por lo tanto, no podrán nunca definirse como datos no personales desde el principio. Lo anterior porque hay datos que no necesariamente lo harán, solo bajo ciertas circunstancias y/o medios empleados, los cuales únicamente evidenciarán información personal de manera extrínseca. A continuación, ejemplos y un detalle de lo que postula Janeček (2018) son los siguientes:

- Datos intrínsecamente personales: estos revelan la información personal y controlarlos es casi como hacerlo con la identidad individual, su retención invade, sin más justificación, el derecho humano fundamental a la protección de datos personales y la privacidad o hasta intimidad. Un ejemplo, en la jurisprudencia del Tribunal Europeo de Derechos Humanos

[15] Un ejemplo de esta idea es el tratamiento especial otorgado, por distintos ordenamientos jurídicos, a los datos personales sensibles. En la LPDP (2011), el consentimiento debe ser por escrito y se generan mayores obligaciones para resguardar su seguridad y confidencialidad, pues su naturaleza lo justifica.

[16] Cabe destacar que este análisis fue realizado para determinar la viabilidad de promover un régimen "análogo" al de propiedad para fomentar el control, vía un régimen de derechos de exclusividad como los existentes en otras áreas del derecho, sobre datos que no son personales y sobre datos que el autor califica como "extrínsecamente personales". Esta propuesta, evidentemente, separa el componente personal de dichos datos, ya que la propiedad no puede existir sobre derechos personales.

[TEDH] y, en Perú, sería una secuencia de ADN humano o muestras de células humanas, los cuales son datos sensibles por ser relativos a la salud.

- Datos extrínsecamente personales: ejemplos de estos serían los datos de GPS, una dirección IP compuesta por metadata o los datos almacenados en un administrador de tareas personal. Estos lo son solo extrínsecamente; por ende, cuestiones éticas y legales, mencionadas en el caso anterior, no le serán necesariamente aplicables.

En la práctica, la solución que viene siendo aplicada por diversos ordenamientos jurídicos, es establecer una definición de dato personal desde el significado de los mismos, es decir, desde la información. Además, delimitan un régimen de protección para el tratamiento de los datos personales, encontrando balances entre la mencionada "teoría de la dualidad de los datos", es decir, que incorpora elementos de ambos enfoques[17], al momento de configurar los elementos de dicho régimen: en las definiciones, derechos, obligaciones, excepciones, graduaciones y demás disposiciones legales.

Por ello, como Rauhofer y Lynskey (2019) señalan, resulta económicamente valioso el otorgar derechos a las personas sobre sus datos; además, el equilibrar estas perspectivas, permite a los reguladores combinar los objetivos económicos y la generación de confianza en las tecnologías digitales y el procesamiento de datos personales[18]. Sin duda, la práctica regulatoria mundial es una prueba de ello.

[17] Un claro ejemplo es el Reglamento UE 2016/679, Reglamento General de Protección de Datos Personales [RGPDP] (2016). Véase la parte considerativa y el artículo 1º que define su objeto.

[18] Un caso de objetivos que sirven a ambos enfoques, entre varios otros, como señala Lynskey (2015),está relacionado a los requisitos de transparencia incorporados en el RGPDP (2016) para reducir las asimetrías de información entre los individuos y las organizaciones. Con ello, el riesgo de que los individuos estén sujetos a daños tangibles o intangibles. Otros ejemplos en el RGPDP (2016) se pueden encontrar en los derechos otorgados a los titulares de los datos personales, como lo son el derecho al olvido y el derecho a la portabilidad de datos personales, ya que contribuyen a fortalecer el control del individuo como actor en el mercado, entre otros efectos que serán analizados posteriormente.

Considerando lo anterior, el legislador nacional optó por la siguiente definición de dato personal: "toda información [numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo] sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados" (numeral 4 del artículo 2º, LPDP, 2011). Esta definición es compatible (y casi idéntica) a la citada, líneas arriba, yelaborada por la OCDE (2019a): "Personal data means any information relating to an identified or identifiable individual (data subject) [dato personal significa cualquier información relacionada con un individuo identificado o identificable (titular de los datos personales)]" (p. 7).

Asimismo, un dato personal posee (4) cuatro elementos o componentes que, entre ellos, están "estrechamente ligados y se complementan recíprocamente" (Grupo de Trabajo del Artículo 29°, 2007, p. 6):

- Información: Purtova (2018), como crítica al RGPDP (2016) y aplicable en sede nacional, menciona que este otorga un amplio margen sobre los alcances de la protección de dato personal, definiendo este concepto, desde el término información. Sin embargo, no establece ningún significado legal sobre lo que debe entenderse por información y únicamente se enumeran (múltiples) clasificaciones de datos que califican como personales.

  La definición en la LPDP (2011) es amplia al incluir el término "[t]oda información" (numeral 4 del artículo 2º, Ley Nº 29733, Ley de Protección de Datos Personales, 2011), ya que evita ser restrictiva en sus demás disposiciones. Por su lado, el Reglamento (2013), también, define al dato personal desde el plano de la información, mencionando distintas clasificaciones como "aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo". Esto ocurre al definir a los datos personales relacionados con la salud[19] y

[19] "(…) aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética" (Numeral 5 del artículo 2º, Reglamento, 2013).

los datos sensibles[20], pero, nuevamente, sin establecer qué significa la información.

Sin duda, la anterior autora se acerca a lo anticipado por Janeček (2018) y la OCDE (2019a). Concluye que una definición tan amplia de dato personal y poco delimitada genera zonas grises y, hoy en día, con miras al futuro del Big Data y de la IoT, todo dato puede considerarse como de carácter personal al hacer identificable con otros medios razonablemente usados, a una o varias personas naturales e incidir directamente en la vida de los individuos. Por ello, si la tendencia es que inevitablemente todos los datos acaben dentro del ámbito de los datos personales, una solución podría ser abandonar la distinción entre datos personales y no personales en aras de adoptar el principio de que todo procesamiento de datos debe activar protección. Además, podría trabajarse en cómo aplicar dicha protección a distintos sectores o situaciones específicas.

Así, no es necesario que la información sea verídica o esté probada. Podría ser incorrecta. Prueba de ello son los derechos de actualización, inclusión, rectificación, supresión y/o cancelación otorgados al titular de los datos personales. De igual modo, el formato o soporte de cómo está contenida la información, puede ser cualquiera. La LPDP (2011) menciona que el tratamiento puede ser por medios automatizados, manuales y/o ambos.

- Identificabilidad (hacer a un sujeto identificado o identificable): este elemento parte de la idea de que una persona natural es identificada cuando, dentro de un grupo de personas, se la distingue de todos los demás miembros del grupo; y, es identificable cuando, aunque no se la haya identificado

[20] Definido de la siguiente manera:

> Información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad" (Numeral 6 del artículo 2º, Reglamento, 2013).

todavía, sea posible hacerlo (Grupo de Trabajo del Artículo 29, 2007; Purtova, 2018).

La legislación europea menciona que la identificación se logra normalmente a través de datos concretos denominados identificadores, que tienen una relación privilegiada y muy cercana a una determinada persona[21]. Estos, a su vez, pueden identificar o hacer identificable a alguien de forma directa o indirecta.

El Grupo de Trabajo del Artículo 29 (2007) destaca que, en la forma directa, a través de los identificadores, la información original se asocia con una persona física que puede ser distinguida de otros individuos. La forma indirecta se refiere a las combinaciones únicas, pequeñas o grandes; si a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, esta aún puede ser identificable porque esa información, combinada con otros datos (tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras.

Finalmente, dicho equipo señala que la identificación, a través del nombre y apellidos es lo más habitual, pero puede no ser necesaria para identificar. Por ejemplo, cuando los ficheros informatizados de datos personales asignan un identificador único a las personas registradas o las herramientas de control de tráfico en Internet permiten conocer el comportamiento de una máquina y, por tanto, la del usuario detrás, incluyéndola en una categoría sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y le atribuyen determinadas decisiones (p. 15).

[21] Se considerará persona física identificable toda aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (numeral 1 del artículo 4º del RGPDP, 2016).

De esta manera, en la Resolución Directoral Nº 35-2019-JUS/DGTAIPD, la autoridad peruana, refiriéndose al dato personal, advierte como segundo elemento "b) que se trate de una información que permita identificar o hacer identificable al titular del derecho". Cabe acotar que al referirse a los elementos del dato y propiamente al de identificabilidad, no lo disgrega o separa adecuadamente, a diferencia de su análogo europeo. Aún así, sobre la identificabilidad, menciona acertadamente lo siguiente:

> [U]na persona es "identificada" cuando, dentro de un grupo de personas, se la distingue de todos los demás. El identificador más común de una persona es el nombre (nombre propio o nombre de pila y nombre patronímico o apellido) por lo tanto, constituye un dato personal y convierte a la persona en "persona identificada", en algunos casos directamente y en otros con medios fácilmente utilizables[22] (p. 7)

Así, la autoridad peruana resalta sobre esta segunda posibilidad de identificabilidad lo siguiente:

> [U]na persona es "identificable", directa o indirectamente cuando, aunque no se la haya identificado todavía, sea posible hacerlo, porque para establecer la identidad habrá que combinar el nombre con otros atributos (fecha de nacimiento, dirección domiciliaria, fotografía, DNI, entre otros). Sobre la identificación indirecta o individualización, lo que quiere decir, es que una persona puede ser identificada dentro de un grupo colectivo de datos, lo que permite que se tome decisiones que afecten a esa persona, como por ejemplo la publicidad comportamental que se hace a través de [I]nternet.

[22] Cabe resaltar que la autoridad peruana habría también adoptado o, en todo caso, reafirmado que la forma de identificar a una persona es a través de identificadores (datos), siendo que en algunos casosesos datos son identificadores directos, pero, en otros, identificadores indirectos o con medios fácilmente utilizables. Como se observa líneas arriba, este análisis coincide en gran magnitud con el realizado con la autoridad europea.

Con ello, se puede dejar en claro que, sobre la posibilidad relevante de identificación en la legislación peruana, la LPDP (2011) dispone como estándar a los medios que pueden ser razonablemente utilizados. No obstante, el problema es que, más allá de lo expresado en dicha Resolución Directoral Nº 35-2019-JUS/DGTAIPD, ni la LPDP (2011) ni su Reglamento (2013) detallan qué debe entenderse por dicha expresión: ¿razonablemente utilizados por cualquiera? ¿Por el responsable del tratamiento en específico o cada situación en concreto? ¿Debería haber algún estándar de medios razonablemente utilizados según cada sector de la industria al que pertenezca el responsable del tratamiento o para cada finalidad específica del tratamiento realizado? Muchas son las dudas que aparecen al momento de aplicar expresiones inconclusas como esta.

Al no haber mayores luces en el plano nacional, se recurrirá nuevamente a la legislación europea que fue ampliamente citada en el documento de Exposición de Motivos del Proyecto de Ley 04079/2009-PE, que dio origen a la LPDP (2011). Al respecto, cabe mencionar que el considerando 26 del RGPDP (2016) tiene un texto similar al nacional, pues indica que debe existir una "probabilidad razonable de que se utilicen medios para identificar a una persona física". Sobre ello, el Grupo de Trabajo del Artículo 29 (2007) indica que, para determinar si existe una probabilidad, es razonable que se utilicen medios para identificar a una persona física; deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

Además, tal Grupo de Trabajo del Artículo 29 (2007) señala que la sola e hipotética posibilidad de singularizar a un individuo no es suficiente para considerar a la persona como identificable. En palabras de dicha entidad, debe analizarse el "conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona", considerando todos los factores en juego como lo costoso de la identificación, la finalidad del tratamiento, la manera en que el tratamiento

está estructurado, el rédito que espera obtener el responsable del tratamiento, los intereses individuales en juego, el riesgo de que se produzcan disfunciones organizativas (por ejemplo, un quebrantamiento del deber de confidencialidad) y los fracasos técnicos.

Purtova (2018) opina que el Grupo de Trabajo del Artículo 29 sigue de cerca el lenguaje del considerando 26 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, vigente al momento de la promulgación de la LPDP (2011). Esta norma derogada (y su considerando) es la que tuvo como guía el legislador peruano.

Además, dicha autora reitera que los medios de identificación tienen posibilidades razonables de ser utilizados, tanto por el responsable del tratamiento como por cualquier otra persona. Este es un enfoque denominado absoluto u objetivo, que permite que más datos se terminen considerando como personales, opuesto al enfoque relativo, que implica interpretar más restrictivamente, tomando en cuenta solo al responsable del tratamiento.

Este estándar resultante de la probabilidad razonable de identificación es bastante amplio y dependiente del contexto, lo que lleva a la consecuencia ya mencionada: el estado de los datos como personales es dinámico. Es posible que el mismo conjunto de datos no sea identificable individualmente al inicio del procesamiento o desde la perspectiva del responsable del tratamiento, dadas las herramientas y los datos disponibles para él. Sin embargo, puede variar desde la perspectiva de otra persona o una vez que las circunstancias cambien por lo que el sistema debe ser capaz de adaptarse a los progresos tecnológicos a medida e introducir las medidas técnicas y organizativas apropiadas a su debido tiempo (Grupo de Trabajo del Artículo 29, 2007; Purtova, 2018)

Como se dijo anteriormente, la autora y otros como, por ejemplo, Narayanan[23], sostienen que una distinción significativa entre información identificable y no identificable no es sostenible por mucho tiempo[24]. La capacidad de re-identificación está aumentando cada año y, aunque la identificación perfecta todavía puede seguir siendo un mito de hoy (Purtova, 2018), en varios casos, la tecnología cada vez más permite medios más eficientes de identificación e impactar en las tomas decisiones de manera granular.

Así, deben tomarse en cuenta las posibilidades de disociación y anonimización contenidas en la LPDP (2011). Ambos conforman un tratamiento de datos personales que impide la identificación o no hace identificable al titular de estos; el primero de forma reversible, mientras que el segundo de forma irreversible. Dada la flexibilidad y adaptabilidad al contexto tecnológico del concepto de dato personal, los procesos de re-identificación tecnológica y la falla en la anonimización de los datos personales se deben tener siempre bajo revisión y no ser tratados como criterios absolutos. Por ello, para varios autores como Purtova (2018), la data disociada sigue siendo información perteneciente a una persona identificable y debería sujetarse a la misma protección del resto de datos personales.

- "Relativo a" o "sobre": la información puede relacionarse con un individuo en contenido, finalidad o resultado. Nótese que estos tres (3) elementos son alternativos y no acumulativos (Grupo de Trabajo del Artículo 29, 2007, pp. 10-11). Sobre el elemento contenido se señala lo siguiente:

[23] Para mayor información ver: http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

[24] Para la autora, esta conclusión es reforzada por el dictamen complementario del Grupo de Trabajo del Artículo 29 (2007) sobre la anonimización: los datos son no identificables, es decir, anónimos, si la anonimización es irreversible. Por ello, afirmarla resulta cada vez más complejo e inexacto.

> [P]roporciona información sobre una persona concreta, independientemente de cualquier propósito (…) o de la repercusión de esa información en el interesado. La información versa «sobre» una persona cuando «se refiere» a esa persona, lo que debe ser evaluado teniendo en cuenta todas las circunstancias que rodean el caso (Grupo de Trabajo del Artículo 29, 2007, p. 11).

Se postulan los siguientes ejemplos sobre el contenido: 1. los resultados de un análisis médico que se refieren claramente al paciente. 2. La información contenida en el expediente de una empresa bajo el nombre de determinado cliente que se vincula (claramente) a él.

Así, la finalidad implica que los "datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona" (Grupo de Trabajo del Artículo 29, 2007, p. 11). Por tanto, en los dos (2) ejemplos anteriores, también podría aducirse que constituyen datos personales, en base a la finalidad por la que se recopilaron y tratan.

Sobre el elemento denominado resultado, Purtova (2018) advierte que gran parte de la información se procesa por las empresas, específicamente, con la intención de impactar a las personas de la manera que describe el Grupo de Trabajo del Artículo 29 (y expuesta en el párrafo anterior), ya que el influir en el comportamiento humano es el principal motivo de la recopilación y procesamiento de la información en Internet. Por ello, la imprevisibilidad de los resultados es siempre uno de los rasgos característicos del análisis de datos avanzado y contraria al principio de limitación de propósito de la protección de datos; por tanto, es innegable que toda la información, en el contexto del negocio de análisis basado en datos, se relaciona con las personas en razón del impacto.

Finalmente, es importante precisar que una misma información, claramente, "puede referirse al mismo tiempo a diversas personas, en función del elemento que esté presente en relación con cada una de ellas" (Grupo de Trabajo del Artículo 29, 2007, pp. 12). Por ejemplo, "a Fulano debido al elemento de 'contenido' (…) y a Mengano si consideramos el elemento de 'finalidad' (la información se utilizará para tratar a Mengano dedeterminada manera), pero también se refiere a Zutano debido al elementode 'resultado' (es probable que la información repercuta en los derechos e intereses de Zutano)" (Grupo de Trabajo del Artículo 29, 2007, pp. 12-13).Por ende, no es necesario que los datos se centren en una persona determinada para considerar que se refieren a ella.

- Vinculación a una persona natural: se define expresamente que el titular de los datos personales es la "persona natural a quien corresponde los datos personales" (numeral 19 del artículo 2º, LPDP, 2011). Esto coincide con la legislación europea, al afirmar que "[l]os datos personales son, por lo tanto, datos relativos a seres vivos identificados o identificables en principio" (Grupo de Trabajo del Artículo 29, 2007, p. 24).

  Así, la información relativa a personas fallecidas no son datos personales bajo la óptica de la LPDP (2011), pues en el derecho civil los fallecidos no son personas naturales o seres vivos, como señala el artículo 61º del Código Civil Peruano al afirmar que "[l]a muerte pone fin a la persona".

  También, se aprecia que el artículo 14º del Código Civil dictamina que "[l]a intimidad de la vida personal y familiar no puede ser puesta de manifiesto sin el asentimiento de la persona o si esta ha muerto, sin el de su cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en ese orden". Si bien el Código Civil otorga cierta protección extensa y superficial, que podría ser de aplicación llegado el momento, la *ratio legis* parece ir más orientada a proteger la intimidad de la vida personal y familiar de los otros miembros de la familia que permanecen en vida y, a su vez, como una protección a lo que se conoce como la personalidad pretérita o memoria de los muertos. A ello, Cárdenas (2020) añade lo siguiente:

> [N]o es que los muertos cuenten con derechos de por sí, sino en tanto su condición pretérita de personas; los tienen en forma limitada, restringida, sin poder ejercerlos por sí mismos, por cierto, pero derechos, al fin y al cabo, como una prolongación trascendente de su personalidad y sobre la base de una dignidad póstuma que tiene el ser humano (p. 192).

Finalmente, Rubio señala que "hablar de derechos de los muertos no es técnicamente exacto, pues solo las personas los tienen; pero vale el término si lo que quiere decirse con él es que tenemos derechos que se ejercen luego de haber muerto" (como se cita en Cárdenas 2020, p. 192).

Respecto a la posibilidad de aplicar la protección de datos personales antes del nacimiento de la persona, el Grupo de Trabajo del Artículo 29 (2007) señala que depende básicamente de cuál sea la posición general de los ordenamientos jurídicos nacionales respecto a la protección del *nasciturus* (el concebido, pero no nacido). Para ello, Rubio insiste en que debe tenerse en cuenta ese posicionamiento general del ordenamiento jurídico nacional junto con la idea de que la finalidad de las normas de protección de datos es proteger a las personas como tal.

En ese sentido, el artículo 1° del Código Civil señala que la "persona humana es sujeto de derecho desde su nacimiento. La vida humana comienza con la concepción. El concebido es sujeto de derecho para todo cuanto le favorece. La atribución de derechos patrimoniales está condicionada a que nazca vivo".

Por otro lado, respecto a la posibilidad de que las personas jurídicasalcancen dentro de esta protección, el documento de Exposición de Motivos del Proyecto de Ley 04079/2009-PE, que dio origen a la LPDP (2011), menciona expresamente lo siguiente:

> [E]n cuanto al ámbito subjetivo de tutela del proyecto, este se ha circunscrito a las personas naturales. No ha considerado, en

> consecuencia, a las personas jurídicas. Esto se debe a la decisión de asumir, más bien, una posición conservadora, basados en que la primera alternativa es la que cuenta con mayor número de precedentes en el derecho comparado de la protección de datos personales, pues esta legislación fue pensada inicialmente para proteger la intimidad de las personas naturales (p. 34).

Para concluir, es innegable la importancia de disgregar y tener en cuenta que un dato personal está conformado por cuatro (4) elementos. No obstante, en el plano nacional, como se vio en el elemento identificabilidad, la Dirección de Protección de Datos Personales, en la citada Resolución Directoral Nº 35-2019-JUS/DGTAIPD recoge estos cuatro elementos (y su contenido expuesto) de una forma peculiar, pues menciona que este Despacho advierte dos (2) elementos: "que se trate de información personal y de una información que permita identificar o hacer identificable al titular del derecho" (p. 7). Curiosamente, dentro de estos dos (2) elementos, catalogados así por la autoridad peruana, se percibe una mezcla, en algunos casos, repetitiva, de los cuatro elementos ya explorados: (i) "que se trate" en alusión a "relativo a" o "sobre"; (ii) información; (iii) identificar o hacer identificable en alusión a identificabilidad; y, (iv) personal o titular del derecho[25], en alusión a la persona natural.

1.3 Tipos de datos personales

Como se aprecia, la LPDP (2011) y el Reglamento (2013) otorgan una definición abstracta, abierta y enumerativa sobre qué puede catalogarse como dato personal;

[25] La denominación "titular del derecho" ha sido abandonada por algunas legislaciones como la europea a favor de llamarlo "interesado", en tanto que aludiría a una "titularidad" sobre un derecho,como si este fuera un derecho patrimonial real o, incluso, personal, que en algún punto pudiese serenajenada o cedido por voluntad propia, tal como sucede con derechos regulados en el Código Civilu otros cuerpos normativos subyacentes. No obstante, el titular de los datos personales no es en estricto un titular, más bien todos estos derechos surgen como una protección a la manifestación de su autodeterminación informativa que, a su vez, es uno de los derechos que componen el derecho de la personalidad del ser humano (por ende, su personalidad en sí misma), siendo inalienable y conuna naturaleza distinta a aquellos derechos patrimoniales.

así, los ejemplos de qué califican como datos personales son casi infinitos. Para ello, en la doctrina, la forma en la que se ha venido clasificándolos, tomando en consideración tanto el nivel de abstracción de dicho concepto, como la posibilidad abierta de múltiples ejemplos (conocido en ingles bajo la denominación de *granular effects*), ha sido mediante taxonomías y/o jerarquías que van disgregándose en clasificaciones y/u objetos más concretos, gracias al disruptivo fenómeno de la dataficación[26]. Lo anterior quiere decir que todo (o casi todo) puede ser expresado, trasladado y/o desarrollado mediante datos.

Un segundo factor es que, al tratar de clasificar o diferenciar incluso solo aquellos datos que son personales, podrían emplearse varios criterios como determinantes por su contenido, origen, tipo de tratamiento, forma de almacenamiento, la forma y/o límites del consentimiento otorgado o si media una excepción a la obtención del mismo, entre otras[27]. Por eso, para presentar al lector las categorías, se hará previamente hincapié en la funcionalidad y/u objetivos a alcanzar con cada clasificación propuesta.

La clasificación más básica y reconocida legalmente en la LPDP (2011) y su Reglamento (2013) es la siguiente:

- Datos personales generales abarcan la "información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados" (numeral 4 del artículo 2º, Reglamento, 2013).

[26] Traducción de un fenómeno dado a un formato cuantificado para permitir la organización y el análisis de esos datos (Mayer-Schönberger & Cukier, 2014).

[27] Como ejemplo, la "Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales", aprobada por la Resolución Directoral Nº 019-2013-JUS/DGPDP, que es un instrumento que facilita el cumplimiento de la LPDP (2011), señala que para su elaboración, fue necesario "cruzar criterios que pueden describir y caracterizar los bancos o tratamientos de datos, como son: el tipo de datos (generales o sensibles), el número de datos de cada persona, el número de personas y el tiempo previsto o previsible de uso de la información, entre otros" (p. 6).

- Datos personales sensibles configuran información relativa a los datos personales: "características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad" (numeral 6 del artículo 2º, Reglamento, 2013). Se requiere que el consentimiento sea siempre otorgado por escrito, a través de firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular (artículo 14º, Reglamento, 2013). Así, la subcategoría de datos personales relacionados a la salud entra en esta categoría.

Complementariamente, la Dirección de Protección de Datos Personales [DPDP], para efectos prácticos de declarar las categorías de los datos personales tratados por el titular del banco de datos personales[28], menciona en el numeral II.2 del Formulario TUPA Nº 34 B: Formulario para persona jurídica, Dirección General de Protección de Datos Personales, los siguientes tipos de datos personales sometidos a tratamiento:

- Datos de carácter identificativo[29]: nombres y apellidos, número DNI, número RUC, Nº de pasaporte, carné de extranjería, dirección del domicilio, teléfono, dirección de correo electrónico, imagen, voz, forma, firma electrónica, otros (detallar).
- Datos de características personales: estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos académicos, datos de derechohabientes, datos de persona de contacto, otros (detallar).

---

28 Las denominaciones exactas, según el titular del banco de datos, son las siguientes:

- Formulario TUPA Nº 34 A: Formulario para entidades públicas
- Formulario TUPA Nº 34 B: Formulario para persona natural
- Formulario TUPA Nº 34 C: Formulario para persona jurídica

29 Este mismo criterio ha sido reiterado por la autoridad en la Opinión Consultiva N° 020-2021-JUS/DGTAIPD. Ver su numeral III.14.

- Datos económicos-financieros y de seguros: créditos, préstamos, avales, datos bancarios, historial de créditos, información tributaria, seguros, tarjetas de crédito, bienes patrimoniales, planes de pensiones/jubilaciones, beneficios recibidos de programas sociales, hipotecas, deudas, otros (detallar).

- Datos de carácter social: pertenencia a clubes o asociaciones, aficiones y hábitos personales, características de vivienda, otros (detallar).

- Datos sensibles: origen racial o étnico, convicciones filosóficas o morales, información relativa a la salud física o mental, afiliación sindical, vida sexual, creencias religiosas, información genética, convicciones políticas, huella dactilar, reconocimiento de iris, reconocimiento facial, reconocimiento de retina, otros.

Por otro lado, doctrinariamente, hay otros autores como Abrams (2014), que advierten que los regímenes legales actuales se basan en la presunción de que los datos se recopilan, principalmente, de la persona con cierto nivel de conocimiento. No obstante, cada vez más, los datos no se recopilan directamente del individuo, sino más bien a distancia, sin que el individuo sea consciente de su origen y usos posteriores (p. 2). Por esto, el autor propone una taxonomía desde la forma en que se originan los datos personales y desde el nivel de consciencia que, en la práctica, los propios titulares de los datos personales poseen al ser proporcionados o generados. De este modo, existen cuatro (4) categorías principales: proporcionada, observada, derivada e inferida:

Tabla 1

Categorías de data basados en su origen

Categoría	Sub-categoría	Ejemplos	Nivel de conciencia individual

Proporcionada[30]	Iniciada[31]	Aplicaciones Registros Registros públicos (i.e., archivos y licencias) Compras con tarjeta de crédito	Alto
	Transaccional	Facturas pagadas Las consultas y encuestas respondidas a los registros públicos (salud, escuelas y tribunales)	Alto
	Publicada	Discursos en lugares públicos Publicaciones en redes sociales Servicios de fotos y video	Alto
Observada[32]	Comprometida[33]	Cookies en una página web/ Tarjeta de fidelización Sensores de ubicación activados en dispositivos personales	Medio

[30] Se originan a través de acciones directas tomadas por la persona con pleno conocimiento de las acciones que llevaron al origen de datos.

[31] Son el producto de las personas que realizan una acción que inicia una relación. El individuo es consciente de la acción que está realizando. Si bien el individuo no siempre considera las implicancias exactas, es previsible que sus acciones crearían datos personales.

[32] Los datos observados son simplemente lo que se observa y registra.

[33] Si bien el individuo puede olvidar que se están creando los datos, existe conciencia general de que se está produciendo. En algunos casos, el individuo puede oponerse o detenerlo, por ejemplo, al desactivar el wifi de su dispositivo móvil.

	No anticipada[34]	Datos de la tecnología de sensores en mi coche Tiempo detenido sobre un píxel en la pantalla	Bajo
	Pasiva[35]	Imágenes faciales de CCTV[36] Tecnologías web oscurecidas Lectores de *wifi* en edificios que determinan la ubicación	Bajo
Derivada[37]	Computacional	Ratios de crédito Compra media por visita	Medio a bajo
	De anotación	Clasificación basada en atributos comunes	Medio a bajo
Inferida[38]	Estadística	Puntajes de crédito y fraude Puntuación de respuesta	Bajo
	Avanzada analítica	Riesgo de desarrollar un análisis multifactorial basado en enfermedades	Bajo

[34] Cuando las personas son conscientes de que hay sensores, pero tienen poco sentido de que están creando datos que pueden pertenecer a la persona. Esta subclasificación sería apropiada para muchasde las aplicaciones relacionadas con IoT. Los individuos típicos tendrían un conocimiento limitadode este tipo de datos.

[35] Cualquier situación en la que sería muy difícil para las personas ser conscientes de que están siendo observados y, a partir de este, se están creando datos relacionados.

[36] "Acrónimo para Circuito Cerrado de Televisón (o *Closed Circuit Television*) (…) se trata de una instalación de componentes directamente conectados, que crean un circuito de imágenes que no puede ser visto por otra persona fuera de él" (Tyco Integrated Fire & Security, 2014).

[37] Se genera mecánicamente, a partir de otros datos, y se convierte en un nuevo elemento de datos relacionado con el individuo.

[38] Son el producto de un proceso analítico basado en probabilidades.

	Puntaje de éxito universitario basado en análisis de múltiples variables

Nota. Adaptación de Abrams (2014).

A modo de recuento, Abrams (2014) expone que los datos proporcionados y observados provienen directamente de las contribuciones y las observaciones de los individuos. Los datos derivados e inferidos son el producto del procesamiento de otros datos. Sin embargo, una vez creados, los datos derivados e inferidos se convierten en el material de alimentación para los datos futuros creados por el procesamiento continuo.

Así, Abrams (2014) argumenta que, en los sistemas computarizados, al inicio, los datos personales empiezan siendo proporcionados principalmente por personas de forma directa, ya que esas participaron en el comercio y otras facetas de la vida. No obstante, hoy, cada vez más datos se originan también a partir de observaciones que son menos obvias para el individuo y son producto del procesamiento. Estos nuevos datos son generados por entornos más ricos en sensores y organizaciones que requieren usar procesos analíticos avanzados como el Big Data. En ese sentido, para lograr una gobernanza correcta, se debe comprender de dónde provienen los datos, cómo se crean y qué tan consciente e involucrado está el individuo en su creación.

Para este autor, la conclusión es que los datos generan más datos, se crean cada vez más a distancia y sin la participación del individuo. Los datos tienden a ser el producto de procesos más sofisticados y su aplicación tiene implicaciones más positivas para todas las partes involucradas. Nótese que la aplicación de los datos también crea nuevos riesgos que el individuo no está en condiciones de mitigar, a través de lo que el autor llama los derechos de autonomía, que se encuentran en los ordenamientos jurídicos (pp. 8-9).

Otra taxonomía, ampliamente citada en el medio, es la elaborada por la OCDE (2019a), que combina clasificaciones existentes, como la anterior (Abrams, 2014; Comisión de la Productividad de Australia[39], 2017). Esta identifica ciertos tipos de datos personales, según su forma de obtención:

- Datos ofrecidos voluntariamente (o entregados, aportados o proporcionados): por individuos cuando comparten explícitamente información sobre ellos mismos o sobre otros como, por ejemplo, al crear un perfil de red social y al ingresar información de tarjeta de crédito para comprar en línea.

- Datos observados: capturan y registran las actividades, el papel del interesado es pasivo y el responsable del tratamiento juega el papel activo como, por ejemplo, los datos de ubicación de teléfonos móviles o lo relacionado el comportamiento del uso de la web.

- Los datos derivados (o inferidos o imputados): se crean basándose en el análisis de datos e incluye los mecánicamente creados. El procesador o encargado del tratamiento de datos tiene un rol activo. El sujeto de datos, normalmente, tiene poca conciencia sobre lo que se infiere sobre él o ella como, por ejemplo, los puntajes crediticios calculados en función del historial financiero de una persona. Narayanan y Shmatikov señalan que, en estos casos, la información personal puede derivarse de datos que, aparentemente, son anónimos o no personales (como se cita en OCDE, 2019).

- Los datos adquiridos (comprados o con licencia): se obtienen de terceros en base a contratos de licencia comercial como, por ejemplo, cuando los datos se adquieren de intermediarios de datos u otros medios no comerciales como, son adquiridos a través de iniciativas de gobierno abierto. Así, las obligaciones contractuales y otras legales pueden afectar la reutilización y

[39] La Comisión Australiana de Productividad es un organismo asesor independiente creado con el fin de apoyar las decisiones del primer ministro en materia económica.

el intercambio de datos. El proveedor del producto o tercero con acceso a los datos originales, consiguen los datos para su procesamiento posterior (y la creación de datos derivados) o en una forma menos identificable, con aquellos adquiridos de (otros) terceros.

Como ejemplo de la especialización en un sector específico, se muestra la taxonomía elaborada por ISO/IEC (2017), compuesta por un conjunto de categorías de datos presentes en el ecosistema de dispositivos y servicios en la nube (pp. 17)[40]:

Tabla 2

Categorías de datos en el ecosistema de dispositivos y servicios en la nube

Datos de contenido del cliente[41]	Credenciales[42]
	Listas de contacto de clientes
	Datos de salud personal y registros médicos

[40] Nótese que en el documento elaborado por ISO/IEC (2017) se advierten dos límites. Primero, los objetos de datos en el ecosistema cambian constantemente a medida que la tecnología, los dispositivos y los servicios en la nube evolucionan. Esto somete la lista a una revisión constante. Segundo, la lista de objetos y usos sería tan larga, duplicada y compleja que a las partes interesadasles resultaría difícil obtener una comprensión útil de cómo se gestionan realmente los datos mediantela revisión de una gran cantidad de objetos de datos individuales. Para facilitar la transparencia, losproveedores de servicios en la nube deben describir cómo se procesan y utilizan los datos de la manera más simple posible, utilizando declaraciones que cubran el conjunto más grande y abstractode objetos de datos.

[41] Datos del cliente en el servicio en la nube que se amplían para incluir objetos de datos similares proporcionados a aplicaciones que se ejecutan localmente en el dispositivo. Tomar en cuenta que la aplicación que se ejecuta localmente puede optar por compartir o no esos datos con el servicio en la nube y, sin embargo, los datos aún encajarían en esta definición ampliada.

[42] Datos proporcionados por el cliente para identificar a un usuario en el dispositivo, aplicación o servicio en la nube como contraseñas, sugerencias de contraseña, etc., incluidos si son biométricos.

		Data genética personal
		Data biométrica personal
		Datos personales de niños
		Opiniones políticas
		Detalles financieros
Datos[43] derivados	Información identificable del usuario final	Data telemétrica
		Data de conectividad
		Uso observado de la capacidad del servicio
		Información demográfica
		Datos de perfilamiento
		Datos del consumo de contenido
		Historial de navegación de la perspectiva/lado del cliente
		Comando de búsquedas y consultas
		Ubicación del usuario
		Data social[44]

[43] Cuando un usuario utiliza las funciones de una aplicación que se ejecuta localmente en el dispositivoy esta parte local de los datos se transmite al servicio en la nube, se convierten en datos derivados del servicio en la nube.

[44] Estos datos se refieren a registros de interacción entre el usuario, otras personas y organizaciones. Incluye listas de amigos e información sobre tipos de interacciones.

	Data biométrica y de salud
	Data de contacto del usuario final
	Data de sensor ambiental del usuario[45]
	Información identificable de organización[46]
Data del proveedor de servicios en la nube[47]	Data de acceso y autenticación[48]
	Data de operaciones[49]
Data de cuenta[50]	Información de contacto o de administración de la cuenta

[45] El entorno físico capturado por los sensores cuando el usuario ejerce una aplicación o las capacidades del servicio en la nube.

[46] Datos que se pueden usar para identificar a un poseedor o locatario en particular (configuración general o datos de uso). No es que se pueda vincular a un usuario específico porque no contiene datos de contenido del cliente; incluye los datos agregados de los usuarios de un locatario que no pueden vincularse al usuario individual.

[47] Data exclusiva del sistema y bajo el control del proveedor de servicios en la nube. No incluye datosde contenido del cliente ni datos derivados.

[48] Utilizados dentro del servicio en la nube para administrar el acceso a otras categorías de datos o capacidades dentro del servicio. Incluye contraseñas, certificados de seguridad y otros datos relacionados con la autenticación. Los datos de control de acceso son un subtipo de datos del proveedor de servicios en la nube.

[49] Data para respaldar el funcionamiento de los proveedores de servicios en la nube y el mantenimientodel sistema, como registros de servicio, información técnica sobre una suscripción (por ejemplo, topología de servicio), información técnica sobre un locador (por ejemplo, nombre de función del cliente), ajustes y archivos de configuración.

[50] Datos específicos de cada cliente del servicio en la nube que se requiere para registrarse, comprar o administrar el servicio en la nube. Estos datos incluyen información como nombres, direcciones, información de pago, etc. Los datos de la cuenta, generalmente, están bajo el control del proveedor de servicios en la nube, aunque cada cliente del servicio en la nube tiene la capacidad de ingresar, leer y editar los datos de su propia cuenta

Datos del instrumento de pago

Nota. Adaptación de International Organization for Standardization e International Electrotechnical Commission (2018).

Como se aprecia, existen varios criterios para diferenciar a los datos personales. Lo importante es tener en cuenta aquellos en base a los que se pretenderá diferenciar o categorizar a los datos personales. Ahora bien, en los primeros dos (2) casos presentados es claro que, desde el aspecto legal, se busca establecer esferas de protección distintas, según las necesidades y/o naturaleza de cada categoría de dato personal. En el caso de los datos calificados comosensibles, se les brinda un ámbito de protección más elevado, imponiéndose una obligación mayor de recabar el consentimiento por escrito, requiriendo medidas técnicas, legales y organizativas más fuertes, debido a que estos sí identifican directamente a la persona natural y pertenecen a la esfera más íntima de la personay/o a sus familiares, de ser el caso.

La relevancia de los siguientes tres (3) modelos es que recogen la práctica económica. Aquí, el uso recurrente de los datos, en su mayoría personales, y la generación de valor agregado a los mismos, se han vuelto esenciales en todo sector, especialmente, en el digital a raíz de algunas particularidades que lo diferencian de los mercados tradicionales[51]. Curiosamente, el uso intensivo de datos se alude como la causa de ciertas consecuencias negativas en dicho mercado digital, como lo son latentes tendencias oligopólicas, monopólicas y de concentración en torno a la prestación de servicios y productos. Por ello, resulta necesario resguardar y regular adecuadamente el régimen de protección de obligaciones/derechos en las áreas implicadas, como lo son el régimen de protección de datos personales, aspectos de consumo, derechos de propiedad intelectual y otros inmersos.

[51] Los mercados tradicionales son espacios que permiten el intercambio de bienes o servicios sin el uso de la tecnología. Por el contrario, uno digital, vía tecnologías digitales, puede facilitar el comercio de bienes o servicios físicos o no.

Todas estas particularidades comerciales evidencian la necesidad de brindar mecanismos de protección más adecuados a las variadas naturalezas de los datos personales, pues son el primer paso para ejercer su control. Además, se apoya en que los titulares de los datos personales tienen un rol activo en el mercado y no solo los responsables del tratamiento de datos personales son quienes participan del aspecto económico. Así, en virtud de una relación jurídica, el primero otorga su consentimiento a cambio de un beneficio comercial-económico. Por ello, en las siguientes secciones, se ahondará en estrategias regulatorias abordadas de forma transversal y articulada con otras áreas del derecho y la práctica comercial (dinamismo, masivo análisis y utilidad esencial en el desarrollo de las actividades económicas); por lo que entender las descritas categorizaciones legales de los datos personales y sus formas de obtención será clave.

1.4 Protección de los datos personales como derecho fundamental

Para explicar el inicio de la tendencia internacional a la protección de datos personales hasta su actual reconocimiento en ordenamientos constitucionales, incluido el peruano, se expondrá cronológicamente sus antecedentes genéricos, desde el reconocimiento del respeto por la dignidad humana hasta la derivación, por un lado, del derecho a la privacidad; y, por el otro, a la intimidad. En el segundo caso, se trata de un derecho fundamental, subjetivo, autónomo, con función facilitadora de otros derechos fundamentales.

1.4.1 El derecho a la protección de datos personales en el plano internacional

Aunque algunos autores como Nieves (2012) afirman que ya existían varias nociones históricas provenientes de la época colonial en Estados Unidos de América que, a su vez, venían de la corona inglesa; consistentes en aforismos con implicancias jurídicas como “a man´s house as his castle [la casa de cada uno es su castillo]”: un principio básico heredado del derecho inglés que confiere al hogar del individuo la máxima protección personal para reivindicar la protección personal del individuo frente al poder del monarca, entre otros ejemplos (pp. 204-208). Recién en el siglo XIX se empieza a reconocer jurídicamente al derecho a la intimidad. En 1890, Louis Brandeis y Samuel Warren publicaron en el Harvard

Law Review (en Estados Unidos) su famoso artículo "The Right to Privacy", a efectos de "cimentar un derecho para hacer frente al hostigamiento por los medios de comunicación social de la época, para guardar reserva respecto de aquel aspecto de la vida personal que legítimamente podía ser excluido de la injerencia de la prensa"[52] (Cerda, 2011, p. 48). Tales autores señalan lo siguiente:

> [E]l derecho a la privacidad es el derecho de toda persona a proteger su integridad psicológica ejerciendo control sobre aquella información que afecta a la personalidad individual por reflejar su propia autoestima, de ahí que el derecho a la privacidad forme parte del derecho más general a la inmunidad de la persona, en definitiva "the right to one´s personality" (Nieves, 2012, p. 213).

Por ello, Brandeis y Warren (1890) enfatizan lo siguiente:

> Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society (…) Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right `to be let alone´.[53] Instantaneous photographs and newspaper enterprise have invaded

---

[52] El caso fue inspirado en un conflicto entre un privado y un medio de comunicación. Como se narra en León (2006), en la Saturday Evening Gazette, se difundieron noticias acerca de Warren, abogado y hombre de negocios. Se comunicó el hecho a su socio Brandeis y fue así que nació la idea de escribir aquellas famosas páginas.

[53] Nieves (2012, p. 206) menciona con respecto a tal derecho defendido por el Juez Cooley:

> Cooley utilizaba esta locución para definir el derecho individual a la inmunidad personal frente a agresiones físicas, 'el derecho de la persona se dice que es el derecho a la completa inmunidad; a ser dejado solo'. Y al analizar los supuestos de violación de la Cuarta y Quinta Enmiendas en los casos de registros y requisas ilegales del domicilio con el objetivo de obtener evidencias suficientes para el procesamiento del acusado (…) alcanza tanto frente a la intromisión ilegal de los agentes del gobierno como frente a la curiosidad lasciva del público en general".

Así, la autora indica que, en 1886, el Tribunal Supremo de los Estados Unidos de América adoptó expresamente la argumentación de Cooley en el caso Boyd v. United States.

> the sacred precincts of private and domestic life [Los cambios políticos, sociales y económicos conllevan el reconocimiento de nuevos derechos, y el common law, en su eterna juventud, crece para responder a las nuevas demandas de la sociedad (…) Los recientes inventos y métodos de negocio llaman la atención sobre el siguiente paso que hay que dar para la protección de la persona, y para asegurar al individuo, lo que el juez Cooley llama el derecho a "ser dejado solo". Fotografías instantáneas y empresa periodística han invadido los recintos sagrados de la vida privada y doméstica] (p. 1).

Seguidamente, tras finalizar la Segunda Guerra Mundial y con la antesala de todas las injerencias dictatoriales y totalitaristas de los gobiernos, se reconoció universalmente, por primera vez, lo siguiente:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (artículo 12, Declaración Universal de Derechos Humanos, 1948).

Aquí nacen distintos grados de protección: a la vida privada (y/o intimidad para algunos traductores), vía su sistematización en tratados internacionales sobre derechos humanos, como aparece el artículo 5º de la Declaración Americana de los Derechos y Deberes del Hombre, y, posteriormente, llevados a constituciones políticas nacionales.

Por su parte, Europa afirmó este derecho en 1950, vía el ConvenioEuropeo de Derechos Humanos (CEDH)[54]. En su artículo 8º indica que toda persona tiene derecho al respeto de su vida privada y familiar, hogar y correspondencia; está prohibida la injerencia en este derecho por parte de una autoridad pública, excepto cuando la injerencia sea conforme a la ley, persiga

[54] Fue redactado el 4 de noviembre de 1950, pero entró en vigor en el año 1953.

intereses públicos importantes y legítimos, y sea necesaria en una sociedad democrática.

Paralelamente, en la jurisprudencia constitucional alemana surgió la teoría jurídica influyente desde finales de la década de 1950, que es la "teoría de las esferas", que, como comenta Alexy, consiste en que el Tribunal Constitucional Federal Alemán concibió una serie de círculos concéntricos, o esferas, delineando diferentes áreas basadas en distintos grados de lo privado (como se cita en González, 2014): la *Individualsphäre*, *Privatsphäre* y *Intimsphäre*. Así, Coronel detalla que el término esfera íntima viene (i) de la palabra alemana esfera y (ii) intimidad deriva del latín *intimus* y evolucionó en otros idiomas para formar palabras que se usan con mayor frecuencia como sinónimos de privacidad, tal cual sucede en el idioma francés *intimité* (Bureau de la Terminologie du Conseil de l'Europe 1995, p. 321), o intimidad en el idioma español (como se cita en González, 2014).

En 1960, el académico estadounidense William L. Prosser publicó un artículo en el que se analizó la posibilidad de reconocer la figura de agravio de privacidad en el derecho consuetudinario gracias a la publicación del artículo previo de Warren y Brandeis, en 1890. Prosser describió el reconocimiento de cuatro tipos de agravio de privacidad: la intrusión en la soledad o reclusión de una persona; la apropiación, con fines comerciales, del nombre, semejanza o personalidad de una persona; la divulgación pública de hechos privados vergonzosos sobre una persona; y, la publicidad que coloca a una persona en una falsa luz ante el ojo público (como se cita en González, 2014, p. 27). Con ello, Pino indica que, en la década de 1960, el término privacidad, en dicho país, adquirió dos significados principales: "desde el derecho civil, como una referencia sintética a un sistema de agravios; y, en el ámbito del derecho constitucional, como derecho de las personas a rechazar injerencias de autoridades públicas" (como se cita en González, 2014, p. 28).

Posteriormente, en febrero de 1974, con el acceso de computadores y desarrollo notorio de la tecnología, el presidente Richard Nixon estableció un Comité del Consejo Nacional sobre el Derecho a la Privacidad. Sin embargo, el presidente dimitió tras las investigaciones del Senado y la divulgación del escándalo de *Watergate,* sobre el uso ilegal de los sistemas de grabación en cinta por parte del primero y sus allegados[55]. En este contexto, como afirma González (2014), el 31 de diciembre de 1974, se adoptó la *Privacy Act* para salvaguardar la privacidad individual del uso indebido de registros federales que regulaba la relación entre ciudadanos y el gobierno, pero no entre privados. Con todo, esta resalta por describir a la privacidad como un derecho personal y fundamental protegido por la Constitución de los Estados Unidos de América, directamente afectado por la recopilación, mantenimiento, uso y difusión de información personal. Con esto, la ley no solo sería asociada a prácticas justas de uso de información, sino también a la nueva privacidad de la información, reconocida en la ley positiva (González, 2014).

Con ello, González (2014) concluye que fue la creciente popularidad mundial del término "privacidad" la que llevó a algunos países europeos no anglófonos a tomar prestada la palabra y utilizarla en el contexto de sus propias investigaciones sobre la protección de las personas y el procesamiento de datos. En otros países, sin embargo, los debates giraron en torno a una terminología diferente, como el francés *libertés* o el sueco *integritet*.

Por su parte, en España, se utilizó predominantemente el término intimidad que, luego, sería importado a varios ordenamientos latinoamericanos. El autor español Murillo De la Cueva señala que "(…) para el Tribunal Constitucional de España la facultad de controlar la información que concierne a determinada persona no solo resguarda el derecho a la intimidad, sino que constituye un derecho fundamental autónomo" (como se cita en Cerda, 2011, p. 55). Así, el

[55] Para mayor información ver: https://historia.nationalgeographic.com.es/a/escandalo-watergate-espionaje-presidencial-estados-unidos_15421

derecho a la autodeterminación informativa se reconoció en base al artículo 18.4 de la Constitución Española de 1978: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de sus derechos". Este hecho, como León (2006) advierte, incidiría en cómo se reconoció el derecho a la autodeterminación informativa por el Tribunal Constitucional peruano, el cual tomó la Constitución Política Peruana, vigente desde 1993, pues mantiene similar redacción a la de su predecesora de 1979, la cual incorporó la protección de la intimidad personal y familiar frente a los servicios informáticos, inspirada a su vez en la entonces reciente Constitución Española.

Sin embargo, la Agencia de los Derechos Fundamentales de la Unión Europea [FRA] y el Consejo de Europa (2018) narran que fue en el estado alemán de Hesse, en 1970, donde se adoptó la primera ley federal sobre protección de datos (*Landesdatenschutzgesetz*). En 1973, Suecia adoptó la primera ley nacional de protección de datos (*Data Lag*). Para finales de la década de 1980, varios estados europeos (Francia, Alemania, Países Bajos y Reino Unido) adoptaron la legislación sobre protección de datos para controlar el procesamiento de información personal.

Después, se establecieron instrumentos sobre protección de datos personales a nivel europeo como el Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este fue el primer instrumento internacional jurídicamente vinculante a sus Estados Miembros[56]. Con esto, la protección de datos personales adquirió un valor diferenciado que no está subsumido en el derecho fundamental al respeto de la vida privada[57].

[56] Su fin es garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente, el derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

[57] Por ejemplo, el 15 de diciembre de 1983, en la "*Volkszählungsurteil*" de la Corte Constitucional Federal de Alemania, se afirmó la existencia de un Informationelleselbstbestimmung (autodeterminación informativa), derivado del derecho fundamental ya reconocido anteriormente

Posteriormente, con la firma del Tratado de Lisboa, el 13 de diciembre de 2007, y entrado en vigor el 1 de diciembre de 2009, se introdujo una base legal explícita para la legislación de protección de datos en el artículo 16º del Tratado de Funcionamiento de la Unión Europea [TFUE][58]. Con ello, entró en vigor, de forma vinculante, para sus estados miembros, la Carta de los Derechos Fundamentales de la Unión Europea[59], la cual adquirió estatus de ley primaria e incluyó, de manera separada, el derecho a la privacidad[60] y al derecho a la protección de datos[61], siendo su contenido el siguiente (Carta de los Derechos Fundamentales de la Unión Europea, artículo 8º, 2009):

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
2. Estos datos se tratarán de modo leal para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento

"*allgemeines Persönlichkeitsrecht"* (derecho general de la personalidad). Así, se indicó que el libre desarrollo de la personalidad requiere la protección del individuo contra la recolección, almacenamiento, uso y divulgación ilimitados de sus datos personales. En este sentido, el derecho fundamental garantiza el derecho del individuo a decidir por sí mismo sobre la divulgación y el uso de sus datos personales (BverfG [Tribunal Constitucional Federal], Urteil [Sentencia] des Ersten Senats [Primer Senado] vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215).

58 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes (TFUE, Artículo 16, 2013).

59 Redactada en 2000 y modificada en 2007.

60 "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones" (Carta de los Derechos Fundamentales de la Unión Europea, Artículo 8º, 2009).

61 En esencia, tal Artículo 8 de la Carta se formula varios años después de la entonces vigente Directiva 95/46/CE, Directiva sobre protección de datos. En ese sentido, el primero incorporó o reconoció a nivel fundamental, la normativa preexistente en dicha Directiva (FRA y Consejo de Europa, 2018).

legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

La FRA y el Consejo de Europa (2018) mencionan que los siguientes derechos se diferencian en su formulación y alcance:

- El derecho al respeto a la vida privada consiste en una prohibición genérica de la injerencia, salvo ciertos criterios de interés general que pueden justificarla. El concepto de vida privada ha tenido una interpretación amplia en la jurisprudencia de diversos países en el sentido de que se aplica a situaciones íntimas, información sensible o confidencial, que podría perjudicar la percepción de la ciudadanía respecto de una persona e incluso aspectos de la propia vida profesional y conducta pública. Sin embargo, la determinación de si existe una injerencia en la vida privada depende del contexto y los hechos de cada caso.

- La protección de los datos personales es un derecho moderno y activo que establece "(…) un sistema con mecanismos de control para proteger a los ciudadanos cuando sus datos personales sean objeto de tratamiento" (pp. 21-22), ya que es más amplio que el derecho al respeto de la vida privada. Esta protección afecta al tratamiento de datos personales, independientemente de la relación que se tenga con la privacidad y sus efectos sobre ella.

  No obstante, el tratamiento de datos personales también puede violar el derecho a la vida privada, pero no es necesario demostrar una violación de ella para aplicar sus normas (pp. 22-23). Por ello, Oostven e Irion (2018) reconocen que es un derecho de tercera generación que, al igual que la privacidad, no es un fin en sí mismo porque su protección contribuye, de manera inherente, a promover otros derechos y libertades fundamentales individuales por lo que ambos tienen una función habilitadora o facilitadora denominada *enabling function*. Al respecto, autores, como Lynsky (2014),

señalan que la protección de datos y la privacidad son derechos separados, pero muy superpuestos. También, mencionan que la privacidad es solo uno de los derechos e intereses protegidos por las normas de protección de datos; sin embargo, dado el poco tiempo de aplicación en contraste con otros derechos, las funciones independientes de protección de datos aún no se han terminado de articular por completo.

1.4.2 Reconocimiento y tratamiento constitucional en el Perú

Debe tenerse en cuenta que "la defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y del Estado" (Constitución Política del Perú [Const.], 1993, artículo 1º). Así, legislativamente, se ha previsto el derecho "[a] que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" (Const. 1993, artículo 2.6º).

Algunos autores, como Castro, critican esta segunda redacción constitucional, esencialmente, por la interdependencia de protección de datos de carácter personal y el derecho a la intimidad, ya que la referencia se realiza solo a una de las facultades del derecho de autodeterminación informativa y la circunscripción como sujetos obligados solo a los servicios informáticos (como se cita en Castillo, 2009).

En esa misma línea, Eguiguren (2004a) señala que tal redacción abarca "este derecho en forma defectuosa e insuficiente, pues solo autoriza expresamente al titular a oponerse a que se suministren informaciones que afecten su intimidad personal y familiar" (p. 177). Por ello, indica que una interpretación literal debe descartarse porque "no incluiría el derecho de la persona a acceder (conocer y recibir) (…) sin esta facultad, mal pueden ejercitarse acciones como solicitar y exigir la rectificación o actualización de datos inexactos o falsos ni, mucho menos, la supresión" (Eguiguren, 2004a, pp. 177-178). Para el autor, esta contingencia sería posteriormente subsanada con la redacción del código de la materia.

Desde otra perspectiva, León (2011) considera que el numeral 6 del artículo 2º de la Const. "se limita, nítidamente, a la intimidad de la vida privada y familiar, que es bien distinta de ese aspecto de la personalidad revelado en la jurisprudencia del Tribunal Constitucional alemán, tres décadas atrás, con el nombre de *informationelle Selbstbestimmung [autodeterminación informativa]"* (p. 2). Concluye que la única vía constitucional correcta de reconocer esta tutela sería el "artículo 3 de la Carta Política, que permite deducir de la dignidad de la persona la necesidad de proteger a esta última frente a los riesgos propiciados por las nuevas tecnologías, (…) el almacenamiento y circulación de la información personal" (León, 2011, p. 2).

Así, indica que el debate nacional debería desenvolverse en los términos de la teoría pluralista, que propugna que:

> [E]xiste un elenco de derechos de la personalidad (intimidad, imagen, nombre, honor, etc.) o en los de su oposición, la teoría monista, de creación alemana, y reinante en la experiencia germana: que mediante la protección constitucional de la dignidad de la persona y del libre desenvolvimiento de la personalidad permiten deducir de esta, en el nivel aplicativo, y según las exigencias del momento, múltiples 'aspectos' individuales a tutelar (León, 2011, p.17).

Además, como se mencionó en la sección anterior, León (2006) considera que la autodeterminación informativa se ha diseminado en la doctrina española, tomando como referente a la jurisprudencia de Alemania y la legislación de la Unión Europea, mas no estrictamente a lo consagrado en la Constitución Española de 1978. De este modo, es completamente falso que el derecho recogido en el numeral 6 del artículo 2º de la Constitución sea la autodeterminación informativa. Así, "¿[c]ómo –me pregunto– un derecho recogido en la Constitución española de 1978, importado a nuestro ordenamiento jurídico desde 1993, va a ser el mismo derecho reconocido por el *Bundesverfassungsgericht* solo en 1983?" (León, 2006, p. 196).

A pesar de ello, para el Tribunal Constitucional (TC) no hay duda de que este artículo reconoce el derecho a la autodeterminación informativa en la legislación peruana. Así, lo ha ratificado y desarrollado en varias sentencias:

- Inicialmente, en el fundamento 3 de la Sentencia 1797-2002-HD/TC, un famoso caso de acción de hábeas data interpuesto por el señor Wilo Rodríguez Gutiérrez, a fin de que se proporcione la información denegada sobre los gastos efectuados por el expresidente Alberto Fujimori Fujimori y su comitiva, tras los ciento veinte (120) viajes al exterior durante sumandato presidencial:

  El derecho reconocido en el inciso 6 del artículo 2° de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7 del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen.

  El TC afirma que tampoco debe confundirse con el derecho a la imagen del inciso 7 del artículo 2° de la Constitución, que protege la imagen del ser humano, derivada de la dignidad de la que se encuentra investido. Ni con el derecho a la identidad personal. Esto significa el derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad. Por su propia naturaleza, el derecho a la autodeterminación informativa es

subjetivo, de naturaleza relacional, pues las exigencias que demandan su respeto, se encuentran, muchas veces, vinculadas a la protección de otros derechos constitucionales. Esta idea es muy similar a la *enabling function* o función facilitadora expresada en la sección anterior, reconocida por la doctrina europea.

Para Castro (2008), con esta sentencia, el TC delimitó el contenido del derecho aludido en el inciso 6 del artículo 2 de la Constitución, al que se le denominó autodeterminación informativa: "[e]n dicha oportunidad, el Tribunal tomó distancia de la identificación entre el derecho a la intimidad y el derecho a la protección de datos personales que venía defendiendo hasta ese entonces" (p. 272).

- Posteriormente, en los fundamentos del 2 al 4 de la Sentencia 04739-2007-PHD/TC, el TC reafirma lo siguiente: el reconocimiento de este derecho y su diferenciación de la intimidad, al ser su objeto de protección distinto, pues este sería preservar la vida privada (no únicamente los derechos de la esfera personalísima), garantizando la facultad de ejercer un control en el registro, uso y revelación de los datos que le conciernen. Esto se anota a continuación:

  > El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal (…) se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras este protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la

> facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen.

- En la Sentencia 00693-2012-PHD/TC de hábeas data contra la Administradora Privada de Fondos de Pensiones Integra (AFP Integra), se solicitó la entrega de todas las copias certificadas del expediente administrativo del denunciante. AFP Integra manifestó, entre otros, que ella no era una entidad administrativa a la que pueda solicitarse tal tipo de documentación. No obstante, en dicha sentencia el TC (2012) ordenó atender el pedido de información, debido a que la información inicialmente brindada fue parcial o incompleta, como se detalla:

  > [E]l derecho a la autodeterminación informativa también supone que una persona pueda hacer uso de la información privada que existe sobre ella, ya sea que la información se encuentre almacenada o en disposición de entidades públicas, o sea de carácter privado. En ese sentido, parece razonable afirmar que una persona tiene derecho a obtener copia de la información particular que le concierne, al margen de si esta se encuentra disponible en una entidad pública o privada.

Por todo ello, Eguiguren (2015) afirma que esta protección constitucional tendría dos (2) dimensiones: (i) una negativa, "facultad que asiste al titular del derecho de prohibir el registro, la difusión y trasmisión de datos referidos a información de carácter personal sensible" (p. 133); y, (ii) una positiva, "facultad del titular del derecho de poder controlar los datos concernientes a la propia persona", que comprende el inspeccionar, verificar, actualizar, corregir y cancelar los datos o informaciones referidas a su persona (p. 133).

Adicionalmente, se advierte que el proceso para proteger el derecho a la autodeterminación informativa es "la Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que

vulnera o amenaza los derechos a que se refiere el artículo 2°, incisos 5)[62] y 6)[63] de la Constitución" (Const., 1993, Numeral 3 del artículo 200º).

Con ello, el artículo 59° de la Ley Nº 31307, Nuevo Código Procesal Constitucional [Nuevo CPC] indica que "el habeas data procede en defensa del derecho de acceso a la información pública reconocido en el inciso 5) del artículo 2 de la Constitución" y, además, en defensa del derecho a la autodeterminación informativa, pero bajo las dieciséis (16) modalidades, enunciadas en dicho artículo[64]. Al respecto, el TC señaló en alusión al artículo 64° de la vigente Ley

---

62 Tal inciso faculta a lo siguiente:

> A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado. (Const., 1993, inciso 5 del artículo 2º).

63 "A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" Const., 1993, inciso 6) del artículo 2).

64 Siendo las siguientes:

- Reparar agresiones contra la manipulación de datos personalísimos, almacenados en bancos de información computarizados o no.
- A conocer (i) y supervisar la forma en que la información personal viene siendo utilizada; (ii) el contenido de la información personal que se almacena en el banco de datos; (iii) el nombre de la persona que proporcionó el dato; y, (iv) el lugar donde se almacena el dato, con la finalidad de que la persona pueda ejercer su derecho.
- A esclarecer los motivos que han llevado a la creación de la base de datos.
- A modificar la información contenida en el banco de datos, si se trata de información falsa, desactualizada o imprecisa.
- A incorporar (i) en el banco de datos información que tengan como finalidad adicionar una información cierta, pero que, por el transcurso del tiempo, ha sufrido modificaciones; (ii) información que tiene como objeto aclarar la certeza de un dato que ha sido mal interpretado; y, (iii) al banco de datos una información omitida que perjudica a la persona.
- A eliminar de los bancos de datos información sensible que afectan la intimidad personal, familiar o cualquier otro derecho fundamental de la persona.

N° 28237, Código Procesal Constitucional, que tiene igual contenido al actual artículo 61° del Nuevo CPC (2021), siendo que ambos permiten la acumulación de "pretensiones de acceder y conocer informaciones de una persona, con las de actualizar, rectificar, incluir, suprimir o impedir que se suministren datos o informaciones", que respecto a la posibilidad sobre si únicamente pueden ejercerse, mediante el habeas data, pretensiones que estén expresamente contenidas en las dieciséis (16) modalidades anteriores, que "las pretensiones en el hábeas data no tienen por qué entenderse como limitadas a los casos que establece la ley. Hay posibilidad de extender su alcance protector a otras situaciones o alternativas (…). La propuesta del artículo 64° es simplemente enunciativa" (Tribunal Constitucional. Expediente Nº 06164-2007-HD/TC, Arequipa, Jhonny Robert Colmenares Jiménez; 21 de diciembre de 2007). En ese sentido, pese a que la ley establece supuestos taxativos, por vía jurisprudencial, se habría abierto dicha posibilidad de ampliar el alcance protector a otras alternativas no contempladas en el artículo 59º del Nuevo CPC (2021).

Finalmente, se aprecia que la autodeterminación informativa comprende, entre otras cosas, lo afirmado en la Sentencia 00693-2012-PHD/TC, en relación a que la persona "pueda hacer uso de la información privada que existe sobre ella" y, por ende, se "tiene derecho a obtener copia de la información particular que le concierne". No obstante, resulta cuestionable e indeterminado si en vía constitucional se podría recurrir a una acción del habeas data para exigir o garantizar la reutilización de la información automatizada que, sobre sí mismo, se trate. Lo anterior no porque no esté comprendido dentro del contenido de este

- A impedir (i) que las personas no autorizadas accedan a una información que ha sido calificada como reservada; y, (ii) la manipulación o publicación del dato en el marco de un proceso, con la finalidad de asegurar la eficacia del derecho a protegerse.
- A que el dato se guarde bajo un código que solo pueda ser descifrado por quien está autorizado para hacerlo.
- A solicitar el control técnico con la finalidad de determinar si el sistema informativo, computarizado o no, garantiza la confidencialidad y las condiciones mínimas de seguridad de los datos y su utilización de acuerdo con la finalidad para la cual han sido almacenados.
- A impugnar las valoraciones o conclusiones a las que llega el que analiza la información personal almacenada.

derecho fundamental, sino porque no lo está en las modalidades enunciadas del artículo 59° del Nuevo CPC (2021). Ello en tanto que la naturaleza del recurso de habeas data tiene como finalidad proteger tal derecho constitucional: "(…) las cosas al estado anterior a la violación o amenaza de violación de un derecho constitucional, o disponiendo el cumplimiento de un mandato legal o de un acto administrativo" (artículo 1°, Nuevo CPC, 2021).

Por ello, como requisito especial, para interponer la demanda de habeas data, el artículo 57.2° del Nuevo CPC (2021) dispone que deben indicarse por qué razones "en el archivo, registro o banco de datos individualizado obra información referida al agraviado; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa, inexacta o violatoria de la intimidad personal o familiar".

Analizando la posibilidad de que dicho tribunal ampare un hábeas data para portar datos personales, si bien, en principio, "las pretensiones en el hábeas data no tienen por qué entenderse como limitadas a los casos que establece la ley" porque "[h]ay posibilidad de extender su alcance protector a otras situaciones o alternativas" (Tribunal Constitucional. Expediente Nº 06164-2007-HD/TC, Arequipa, Jhonny Robert Colmenares Jiménez, 2007), presenta muchas dificultades y limitaciones.

Así, se tendría que probar que no reutilizar de forma directa los datos personales automatizados en los entornos digitales supondrá una concreta violación cada vez que estos deseen ser portados, ya sea por el propio titular de los datos personales o cuando se desee transmitir directamente a otros responsables. Ello en tanto que, como se verá posteriormente, es en grandes rasgos el contenido del derecho a la portabilidad de los datos personales. No obstante, este mecanismo parecería ser contrario a la naturaleza de este derecho y a la inmediatez de los entornos digitales, por lo que este mecanismo no generaría los efectos deseados. Además, se requiere de una serie de medidas técnicas, legales y económicas para su adecuado despliegue, que, difícilmente, podrían ser abordados por cada juez competente en cada caso concreto para la eficacia dela medida en el hipotético caso de que fuese concedida.

Por ello, si bien se ha demostrado suficiente sustento constitucional para el reconocimiento de este derecho, lo más adecuado para garantizar su materialización es contar con una vía legal específica que contemple el reconocimiento del mencionado y una vía definida en la que el responsable del tratamiento o titular del banco de datos deba responder ante su ejercicio.

1.5 Ley de Protección de Datos Personales, su Reglamento, directivas y demás marco regulatorio

A nivel nacional, la LPDP (2011) es la norma aplicable a todos los datos personales contenidos (o destinados a ser contenidos), en bancos de datos[65] personales de administración pública y privada, cuyo tratamiento se realiza en el territorio nacional. Ello con independencia de la modalidad del tratamiento de los datos personales, es decir, "ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren" (artículo 3°, LPDP, 2011). Adviértase que, de existir normas particulares o especiales que incluyan regulaciones sobre datos personales, no excluirán el ámbito de aplicación de la LPDP (2011) y su Reglamento (2013) (artículo 3° del Reglamento, 2013).

De esto se exceptúan en el sector privado a los datos personales contenidos (o destinados a ser contenidos) en bancos de datos personales, creados por personas naturales para fines exclusivamente relacionados con usos domésticos, personales o relacionados con su vida privada o familiar, y entidades del sector público, cuando sea "necesario para el estricto cumplimiento de competencias asignadas por ley (…) que tengan por objeto: la defensa nacional, la seguridad

---

65 Un banco de datos, según el artículo 53º del Nuevo CPC, es lo siguiente:

> (…) archivo, registro, base o banco de datos a todo conjunto de datos organizado de información personal y que sean objeto de tratamiento o procesamiento físico, electrónico o computarizado, ya sea público o privado, y cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Igualmente, el artículo 2.1º de la LPDP (2011) contiene su propia definición, siendo "[un c]onjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso".

pública y, el desarrollo de actividades en materia penal para la investigación y represión del delito" (artículo 3° del Reglamento, 2013).

No debe obviarse que el ámbito de aplicación de la LPDP (2011) es únicamente territorial. Esto difiere con otros ordenamientos jurídicos, como el RGPDP (2016), que es de aplicación a todo tratamiento de datos personales en el extranjero, en tanto estos pertenezcan a ciudadanos europeos. Por ello, deberán observarse, concurrentemente, los siguientes criterios del artículo 5° del Reglamento (2013):

- Que, el tratamiento de los datos personales sea efectuado en un establecimiento en territorio peruano correspondiente al titular del banco de datos personales o del responsable del tratamiento.

- Que, el tratamiento de los datos personales sea efectuado por un encargado del tratamiento, independientemente de su ubicación, a nombre de un titular de banco de datos personales establecido en territorio peruano o del responsable del tratamiento.

- Que, el titular del banco de datos personales o el responsable del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana por disposición contractual o del derecho internacional.

- Que, el titular del banco de datos personales o quien resulte responsable no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que sea con fines de tránsito y no impliquen tratamiento.

Nótese que, cuando el titular del banco de datos personales o el responsable del tratamiento no se encuentre en territorio peruano, pero su encargado sí, le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Reglamento (2013). En caso las opciones del artículo 5° del Reglamento (2013) no brindaran solución para determinar la dirección del domicilio, se considerará con domicilio desconocido en territorio peruano.

Segundo, la LPDP (2011) reconoce principios rectores que le sirven de criterios interpretativos y al Reglamento (2013) como parámetros "para la elaboración de otras disposiciones y para suplir vacíos en la legislación sobre la materia" (artículo 12°, Ley Nº 29733, LPDP, 2011):

- Legalidad: el tratamiento de los datos personales se hace conforme a lo establecido en la ley y la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos está prohibida.

- Consentimiento: para el tratamiento de los datos personales debe mediar el consentimiento libre, previo, expreso, informado e inequívoco de su titular. No se admiten fórmulas de consentimiento en las que este no sea expresado de forma directa, expresa y clara.

- Finalidad: los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita no pudiendo extenderse el tratamiento a otra finalidad distinta.

- Proporcionalidad: todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a su finalidad.

- Calidad: los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados para la finalidad. Estos se deben conservar garantizando su seguridad para cumplir con dicha finalidad. Se presume que los datos directamente facilitados por el titular son exactos[66].

---

[66] Nuestra autoridad peruana, sobre este principio, en el numeral 50 del XI. Análisis del Considerando,en la Resolución Directoral N°1427-2018-JUS/DGTAIPD-DPDP señaló lo siguiente:

> (…) un tratamiento de datos que inicialmente pudo ser lícito - como en este caso - con el paso del tiempo puede dejar de serlo, pues en virtud del `principio de calidad (…) los datos personales (…) deben examinarse no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo tiempo en que se produce este tratamiento (p. 14).

Esto es importante, en tanto se traduce o refuerza en la permanencia del deber del responsable del tratamiento de verificar y de forma constante, hasta que cese el tratamiento, si los datos tratados son

- Seguridad: el titular del banco de datos personales y su encargado deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Estas deben ser apropiadas y acordes con el tratamiento y la categoría de datos personales tratados.

- Disposición de recurso: todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos ante vulneraciones.

- Nivel de protección adecuado: para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, al menos, equiparable a lo previsto por la LPDP (2011) o por los estándares internacionales en la materia.

Como tercer punto, están todas aquellas consideraciones en torno a la forma en que debe obtenerse el consentimiento[67]:

- Informado: conforme al artículo 12.4° del Reglamento (2013) y al artículo 18° de la LPDP (2011), implica dar a conocer clara, expresa e indubitablemente, con lenguaje sencillo, al menos la identidad y dirección del titular del banco de datos personales o responsable a dirigirse para revocar su consentimiento o ejercer sus derechos; la finalidad o finalidades del tratamiento de sus datos personales; la identidad de los que son o pueden ser destinatarios; la existencia del banco de datos personales en que se almacenarán; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga; las consecuencias de proporcionar o no, sus datos personales; y, la transferencia nacional e internacional que se efectúen.

adecuados, pertinentes, actualizados y necesarios para la finalidad para la cual fueron inicialmente recopilados, bajo perjuicio de caer en un tratamiento ilícito.

[67] Para un contraste directo con las condiciones aplicables a las condiciones del consentimiento, sugerimos revisar el artículo 7º del RGPDP (2016), el cual tiene mucha similitud con nuestro marconormativo. Para mayor información: https://gdpr-info.eu/art-7-gdpr/.

- Libre: el artículo 12.1° del Reglamento (2013) indica que el consentimiento se otorgará sin que medie error, mala fe, violencia o dolo en la manifestación de voluntad. Si bien entregar obsequios o beneficios con ocasión del consentimiento no afectan la condición de libertad, si lo hará en menores de edad. Sin embargo, el condicionar la prestación de un servicio, la advertencia o amenaza de denegar el acceso a beneficios o servicios que normalmente son de acceso no restringido, sí afecta la libertad si los datos solicitados no son indispensables para la prestación de dichos beneficios o servicios[68].

- Previo: con anterioridad a la recopilación de los datos.

- Expreso e inequívoco: manifestar el consentimiento en condiciones que no admitan dudas. También, es consentimiento expreso la conducta del titular en tanto se pueda evidenciar indubitablemente que lo ha hecho de forma inequívoca, pues de no hacerlo su conducta sería contraria[69]. En el entorno

[68] Sobre el particular, el RGPDP (2016) indica que la libertad significa que el individuo debe tener libertad de elección. Esto coincide con la normativa peruana. Aquí, se señala que no se debe poneren desventaja al titular de los datos personales, en caso no dé su consentimiento o lo retire posteriormente.

Para ello, el Grupo de Trabajo del Artículo 29 (2018) ha establecido cuatro (4) factores para determinar si el consentimiento se otorga libremente: (i) desequilibrio de poder (el consentimiento no es válido si existe un desequilibrio de poder entre el interesado y el controlador, como la relación entre un empleado y un empleador); (ii) condicionalidad (los controladores de datos no deben vincular las solicitudes de consentimiento para el procesamiento de datos no esenciales a los términos y condiciones de un servicio); (iii) disociación de los fines del tratamiento de los datos (cuando el procesamiento de datos tiene múltiples propósitos, se debe otorgar el consentimiento para cada propósito); (vi) perjuicio (el interesado debe negar su consentimiento sin desventajas, incluidas la intimidación o la coacción; tampoco, debería experimentar una reducción de la calidad de los bienes o servicios, debido a su decisión de no dar su consentimiento).

[69] El Grupo de Trabajo (2018) es aún más específico respecto de la manifestación de voluntad en línea:

> El RGPDP establece claramente que el consentimiento requiere una declaración del interesado o una clara acción afirmativa, lo que significa que siempre debe darse el consentimiento mediante una acción o declaración. Debe resultar evidente que el interesado ha dado su consentimiento a una operación concreta de tratamiento de datos (…). Un responsable del tratamiento debe tener también en cuenta que el consentimiento no puede

digital[70], se considera expreso el hacer clic, cliquear, pinchar, dar un toque, *touch* o *pad* u otros similares mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no. Asimismo, podrá otorgarse mediante firma electrónica o escritura quequede grabada y pueda ser leída e impresa o que, por cualquier otromecanismo o procedimiento establecido, permita identificar al titular y recabar su consentimiento, a través de texto escrito.

Cabe mencionar que existen trece (13) excepciones respecto de la obtención del consentimiento en el artículo 14° de la LPDP[71] (2011). En caso de mediar una de estas limitaciones, ello no limitará el cumplimiento de otras obligaciones como el deber de informar; realizar el flujo transfronterizo de datos personales, solo si el país destinatario mantiene niveles de protección adecuados (salvo que sea de

---

obtenerse mediante la misma acción por la que el usuario acuerda un contrato o acepta los términos y condiciones generales de un servicio. La aceptación global de los términos y condiciones generales no puede considerarse una clara acción afirmativa destinada a dar el consentimiento al uso de datos personales. El RGPDP no permite que los responsables del tratamiento ofrezcan casillas marcadas previamente o mecanismos de exclusión voluntaria que requieran la intervención del interesado para evitar el acuerdo [subrayados añadidos] (por ejemplo, "casillas de exclusión voluntaria") (pp.17-18).

[70] El Grupo de Trabajo (2018) precisa además que, respecto al consentimiento por medios electrónicos, "(…) la solicitud no deberá perturbar innecesariamente el uso del servicio para el quese presta", conforme detalla el considerando 43 del RGPD. "Una acción afirmativa por la cual el interesado indique su consentimiento puede ser necesaria cuando una manera menos invasiva o molesta pudiera dar lugar a ambigüedad". No obstante, adviértase que continuar con el uso normalde un sitio web "(…) no es una conducta de la que pueda inferirse una indicación de que el interesadodesee manifestar su acuerdo con respecto a una operación de tratamiento propuesta" (pp. 18-19).

[71] Para efectos del presente trabajo, únicamente es pertinente mencionar, entre otras, las estipuladas en el numeral quinto del artículo 14º de la LPDP (2011):

> [c]uando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.

Y, a lo dispuesto en el numeral octavo, "[c]uando se hubiera aplicado un procedimiento de anonimización o disociación".

aplicación alguno de los casos exceptuados del artículo 15º de la LPDP); y, respetar el ejercicio de los derechos de los titulares de los datos personales y otras.

Como cuarto aspecto, por tratamiento debe entenderse de la siguiente manera:

> Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales (numeral 19 del artículo 2º, LPDP, 2011).

El tratamiento puede ser llevado a cabo por el responsable del tratamiento[72], el cual puede contar tanto con un encargo de tratamiento[73] como con una subcontratación[74].

Finalmente, el quinto punto, es que el titular de datos personales goza de los siguientes derechos:

- Información: el alcance de derecho ya fue detallado al describirse cómo debe obtenerse el consentimiento para que sea considerado como informado. Se encuentra definido en los artículos 18º de la LPDP (2011), el numeral 4 del artículo 12º y 60º del Reglamento (2013).

---

[72] "Aquél que decide sobre el tratamiento de datos personales, aun cuando no se encuentren en un banco de datos personales" (numeral 14 del artículo 2º, Reglamento, 2013).

[73] "Otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídicaque le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sinla existencia de un banco de datos personales" (numeral 10 del artículo 2º, Reglamento, 2013).

[74] También, existe la subcontratación del tratamiento, si este es realizado por un tercero diferente al encargado del tratamiento, al mediar un convenio o contrato entre estos dos últimos; para ello, se requerirá de manera previa una autorización por parte del titular del banco de datos personales o, de ser el caso, del responsable del tratamiento y el tratamiento que haga el subcontratista, se realizará en nombre y por cuenta del responsable del tratamiento, pero la carga de probar la autorización le corresponderá al encargado del tratamiento (artículo 36º, Reglamento, 2013).

- Acceso: contenido en los artículos 19° de la LPDP (2011) y 61º del Reglamento (2013). Implica obtener información que sobre sí mismo sea objeto de tratamiento en bancos de datos públicos o privados; la forma en que se recopilaron sus datos; las razones que lo motivaron; a solicitud de quién se realizó tal recopilación; las transferencias realizadas o previstas; la información relativa a sus datos personales[75]; y, todas las condiciones y generalidades del tratamiento a estos.

- Actualización: conforme al artículo 20° de la LPDP (2011) y 64º del Reglamento (2013) permite, en vía de rectificación, actualizar aquellos datos modificados a la fecha del ejercicio del derecho.

- Rectificación: el artículo 65° del Reglamento (2013) indica que se pueden modificar los datos inexactos, erróneos o falsos en alusión a este derecho.

- Inclusión: en vía de rectificación, el artículo 66° del Reglamento (2013) permite que los datos personales sean incorporados a un banco de datos personales o al tratamiento, cuando aquella información sea faltante, incompleta, omitida o eliminada en atención a su relevancia para ello.

- Supresión o cancelación: ello procederá, según el artículo 67° del Reglamento (2013), cuando los datos personales hayan dejado de ser, total o parcialmente, necesarios o pertinentes para la finalidad que se recopilaron, si ha vencido el plazo para su tratamiento, o si se revocó el consentimiento o ya no se tratan conforme a la LPDP (2011) o su Reglamento (2013).

---

75 Probablemente, con la expresión: incluye a la información relativa a sus datos personales, se aluda a la metadata sobre los datos personales, es decir, aquellos datos sobre los datos personales, que sirven para suministrar información sobre los datos producidos y consisten en información que caracteriza a los datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos a los que aluden. Lo anterior permite ubicar y entender los datos tratados. Para mayor información ver: https://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos

- A impedir el suministro: conforme al artículo 21° de la LPDP (2011), sobre sus datos personales, especialmente, cuando afecte sus derechos fundamentales. No aplica para la relación entre el titular del banco de datos personales y el encargado de tratamiento.

- Oposición: conforme al artículo 22° de la LPDP (2011) y 71º del Reglamento (2013), se puede oponer al tratamiento de sus datos, si se acreditan motivos fundados y legítimos relativos a una concreta situación personal que lo justifique.

- Al tratamiento objetivo: conforme al artículo 23° de la LPDP (2011) y 72° del Reglamento (2013), implica no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, es decir, busca garantizar que la adopción de dicha decisión no esté sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta. Ahora, existen algunas excepciones a dicho derecho, que son en tanto el titular de los datos personales se encuentre en el marco de una negociación, celebración o ejecución de un contrato o si dicha decisión se adopta con fines de incorporación a una entidad pública, de acuerdo a ley; ello, por supuesto se encuentra sin perjuicio de la posibilidad de defender su punto de vista para salvaguardar su legítimo interés.

- A la tutela: según el artículo 24° de la LPDP (2011) opera si el titular o el encargado del banco de datos personales deniegue al titular de datos personales, total o parcialmente, el ejercicio de sus derechos, pudiendo recurrir a la Autoridad Nacional de Protección de Datos Personales, vía reclamo, o al Poder Judicial, para la acción de hábeas data.

- A ser indemnizado: conforme al artículo 25º de la LPDP (2011) cuando sea afectado por incumplimiento de alguna obligación legal.

1.6 Análisis del derecho de acceso ante la Dirección General de Protección Personales: conclusiones y limitaciones

Como se observó, el marco peruano aplicable a la protección de datos personales incorpora, entre otros derechos, el derecho al acceso de los datos personales. Así, la Autoridad en la Opinión Consultiva Nº 34 -2020-JUS/DGTAIPD ha concluido que este derecho nace de la "facultad de control que tiene el titular del dato personal sobre su información y, por ende, es un derecho personal que se basa en el respeto al derecho de protección de datos" (p. 9). El derecho de acceso, al igual que el resto, está concebido para materializar esa facultad de control, que la autodeterminación informativa implica.

Conforme al artículo 61° del Reglamento (2013), se tiene derecho a obtener del titular del banco de datos personales o responsable, toda la información relativa a sus datos personales, condiciones y generalidades de sus tratamientos. Por ello, como asegura el artículo 63° del Reglamento (2013), esta información debe ser extensa y abarcar todo el tratamiento realizado con respecto al titular de los datos personales independientemente de que se reciba un pedido; siendo el único limitante derechos de terceros.

Un ejemplo de su cumplimiento es la Resolución Directoral Nº RD-044-2015-DGPDP. Aquí, se concluyó que "la información a la que podrá tener acceso el titular de los datos personales debe ser amplia y comprender la totalidad del registro correspondiente al titular del dato personal, aun cuando el requerimiento solo comprenda un aspecto de dichos datos". Esto comprende qué datos se vienen "utilizando, cómo y de dónde fueron recopilados, para qué finalidades se recopilaron, a solicitud de quién se realizó la recopilación, con quién comparten la información, qué transferencias se realizan, en qué condiciones están tratando los datos y cuánto tiempo". En este sentido, a pesar que la reclamada "atendió la solicitud de acceso dentro del plazo, (…) no demuestra que cumplió con el derecho de acceso de acuerdo a la LPDP y su Reglamento, ya que solo indicó que la información de la reclamante la obtuvo de fuentes de acceso al público y que no realiza transferencia de sus datos personales a terceros" (p. 4).

Asimismo, sobre el límite frente a derechos de terceros, en la Resolución Directoral Nº 378-2017-JUS/DGTAIP-DPDP, se afirmó que los datos personales de otros titulares de datos personales e información o documentos de terceros, inclusive si en estos se les alude o impacte, resultan un límite al ejercicio de este derecho. en tanto posee las siguientes características:

> a) La información solicitada debe corresponder exclusivamente a los datos personales del titular, ya que el derecho de acceso es la petición legítima del interesado a obtener información sobre sus propios datos personales y no de "terceros", b) Si bien el derecho de acceso consiste en obtener información de los bancos de datos personales de administración privada o pública, esto no significa el acceso a documentos concretos que puedan contener información de "terceros" como por ejemplo documentos de seguridad de la información (p. 6).

Sobre la legitimidad para su ejercicio[76], los artículos 47°, 48° y 49° del Reglamento (2013) señalan que este derecho solo puede ser ejecutado por el titular de datos personales, sin perjuicio de las normas que regulan la representación. No excluye la posibilidad de ejercer otros derechos, ni será un requisito previo para el ejercicio de los mismos. Su ejercicio se realiza por el titular de datos personales, que acredite su identidad, presentando copia de su Documento Nacional de Identidad (DNI) o documento equivalente[77] (salvo que se use firma digital conforme a la normatividad vigente, en cuyo caso esto sustituye

[76] Por relevancia a esta investigación, los requisitos y demás consideraciones en torno al ejercicio del derecho de acceso, se harán enfocados únicamente al sector privado.

[77] Es de precisar que, para el caso de las entidades de la Administración Pública, esta exigencia no resultaría aplicable en virtud del artículo 5º del Decreto Legislativo Nº 1246, "Decreto Legislativo que aprueba diversas medidas de simplificación administrativo", en tanto tal artículo dispone que las anteriores "están prohibidas de exigir a los administrados o usuarios, en el marco de un procedimiento o trámite administrativo (…) Copia del Documento Nacional de Identidad". En general, en virtud de dicha norma, están prohibidas de exigir a los administrados o usuarios información, como la identificación y el estado civil, que puedan obtener directamente mediante lainteroperabilidad.

la presentación del Documento Nacional de Identidad y su copia); y, mediante representante legal acreditado como tal o representante expresamente facultado, que adjunte copia de su DNI (o equivalente) y acreditación de representación.

Para el contenido de la solicitud, el artículo 50° del Reglamento (2013) indica que debe ir dirigida al titular del banco de datos personales o responsable, conteniendo nombres y apellidos del titular del derecho y acreditación de los mismos y, en su caso, del representante; petición concreta; domicilio o dirección que puede ser electrónica; fecha y firma del solicitante; y, documentos sustentatorios, si se requiriera.

Conforme al artículo 53° del Reglamento (2013), el titular del banco de datos personales o responsable debe contar con un procedimiento sencillo para el ejercicio de los derechos, pudiéndose ofrecer mecanismos adicionales en beneficio del titular de datos personales. No obstante, este será siempre de carácter gratuito, salvo normas especiales de la materia. El ejercicio de los derechos no puede generar un ingreso adicional, ni los medios para el ejercicio de los derechos podrán implicar el cobro de una tarifa adicional al solicitante.

Respecto a los plazos y procedimiento de respuesta[78], todas las solicitudes presentadas deben, en base al artículo 52° del Reglamento (2013), ser recibidas y es necesario dejar constancia de su recepción por parte del titular del banco de datos personales o responsable del tratamiento. Dentro de los cinco (5) días hábiles, desde el día hábil siguiente a la recepción, se requiere revisar el cumplimiento de los requisitos de la solicitud, mencionados en el artículo 50° del Reglamento (2013), y formular las observaciones por incumplimiento que no puedan ser salvadas de oficio. Esto invita al titular a subsanarlas dentro de cinco (5) días hábiles desde su recepción, ya que, de no hacerlo, se tendrá por no presentada la solicitud.

[78] Es de precisar que, independientemente de que se especifique o no, todos los plazos estipulados en la LPDP (2011) y el Reglamento (2013) se computan en días hábiles.

Si la información proporcionada en la solicitud es insuficiente o errónea, de tal forma que no sea posible su atención, el artículo 56° del Reglamento (2013) prevé que se podrá requerir dentro de los siete (7) días hábiles siguientes de recibida la solicitud, la documentación adicional para atender su solicitud que deberá otorgarse en diez (10) días hábiles de recibido el requerimiento, desde el día siguiente de su recepción. En su defecto, se considerará como no presentada. Este plazo de requerimiento adicional está previsto al analizarse el fondo, mientras que el del artículo 52° del Reglamento (2013) estaría concebido para verificar la existencia de los requisitos del artículo 50° del Reglamento (2013), analógicamente, de admisibilidad.

Según el artículo 55° del Reglamento (2013), el plazo máximo para la respuesta al ejercicio del derecho de acceso será de veinte (20) días hábiles, desde el día siguiente de la presentación de la solicitud que, gracias al artículo 57° del Reglamento (2013), podrá ser ampliado por una sola vez, por un plazo de veinte (20) días hábiles más, siempre y cuando las circunstancias lo justifiquen. Debe comunicarse dentro del plazo que se pretenda ampliar.

Conforme al artículo 62° del Reglamento (2013), la información a ser brindada como respuesta, a opción del titular de los datos personales, podrá suministrarse por escrito, por medios electrónicos, telefónicos y de imagen u otro idóneo, es decir, se puede optar por las siguientes formas: visualización en sitio; escrito, copia, fotocopia o facsímil; transmisión electrónica de la respuesta, garantizando la identidad del interesado y la confidencialidad, integridad y recepción de la información; y/o, cualquier otra forma adecuada a laconfiguración o implantación material del banco de datos personales o naturalezadel tratamiento. No obstante, el acceso deberá ser en formato claro, legible e inteligible, sin utilizar claves o códigos que requieran de dispositivos mecánicos para su adecuada comprensión y acompañada de una explicación. Asimismo, debeser en lenguaje accesible al conocimiento medio de la población y los términos que se utilicen. El responsable del tratamiento podrá acordar con el titular el uso de medios de reproducción de la información distintos a los establecidos en el Reglamento (2013) si son más ecológicos.

Finalmente, el artículo 59° del Reglamento (2013) indica que la respuesta total o parcialmente negativa debe estar justificada, señalando el derecho que le asiste a reclamar ante la Dirección General de Protección de Datos Personales. En base a lo anterior, se puede observar que, tanto en la vía constitucional como legal, el derecho de acceso sustenta su naturaleza en el derecho a la autodeterminación informativa e implica obtener información que, sobre sí mismo, sea objeto de tratamiento en bancos de datos personales, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación, a solicitud de quién se realizó la recopilación, y las transferencias realizadas o que se prevén hacer de ellos. Esto es un deber a cargo del titular del banco de datos o del responsable del tratamiento.

Ahora, cuestión distinta es comprender si el derecho de acceso, en los términos regulados, garantiza una adecuada utilización o, para mayor precisión, la reutilización de los datos personales tratados de forma automatizada. Para ello, en la Resolución Directoral N° 1220-2019-JUS/DGTAIPD-DPDP se reitera, en base a la sentencia del TC del Expediente N° 00693-2012-PHDTTC, lo siguiente:

> [E]l derecho a la autodeterminación informativa también supone que una persona pueda hacer uso de la información privada que existe sobre ella, ya sea que la información se encuentre almacenada o en disposición de entidades públicas, o sea de carácter privado.

Por ello, considera que se "tiene derecho a obtener copia de la información particular que le concierne" (pp. 3-4) y "tratamiento similar debe brindarse a la solicitud de escaneo de los documentos" (pp. 3-4). En sí, el derecho de acceso implica no solo el ejercicio o posibilidad de informarse o conocer la información que existe sobre la persona, también garantiza que toda persona pueda hacer uso de su información existente, pudiéndose obtener una copia de lo que le concierna.

Este pronunciamiento lleva a cuestionar si, de cara al avance de la digitalización de distintos sectores de la economía, la forma en que se viene ejerciendo (o se ha previsto su ejercicio) y cómo se atiende tal derecho garantiza su uso por parte del titular de los datos personales. Si bien el artículo 62° del

Reglamento (2013) brinda mucha amplitud y posibilidad para acordar un medio para dar respuesta al derecho de acceso, en caso la vía elegida sea transmisión electrónica, dicha normativa únicamente prevé que deba garantizarse: la identidad del interesado, confidencialidad, integridad y recepción de la información. No obstante, no hay mayores detalles regulatorios que permitan portar la data garantizando su reutilzación. Aun así, el legislador fue oportuno en dejar abierta la posibilidad, en dicho artículo, de poder emplear cualquier otra forma adecuada a la configuración o implantación material del banco de datos personales o naturaleza del tratamiento.

Sin embargo, dado que el Reglamento (2013) impone que el acceso deberá ser "en formato claro, legible e inteligible, sin utilizar claves o códigos que requieran de dispositivos mecánicos para su adecuada comprensión y acompañada de una explicación" (artículo 62º, Reglamento, 2013) y en "lenguaje accesible al conocimiento medio de la población y de los términos que se utilicen" (artículo 62º, Reglamento, 2013) podría generar cierta confusión o alejar la posibilidad de que, por decisión propia o en cumplimiento legal, los titulares del banco de datos personales o los responsables del tratamiento pudiesen entregar la información en formatos que garanticen su reutilización inmediata para otras finalidades, sea por ellos mismos o terceros.

Lo anterior debido a que los formatos que suelen ser considerados como reutilizables en la práctica comercial y legal de varios países, como por ejemplo CSV, JSON y/o XML, si bien permitirán una lectura mecánica inmediata, impedirán que su contenido sea entendido fácilmente por cualquier persona, ya que justamente para que la información sea reutilizada en medios automatizados, se almacena en lenguajes de programación. Lo anterior significa que no cumple con el requisito de contar con un "lenguaje accesible al conocimiento medio de la población y de los términos que se utilicen" (artículo 62º, Reglamento, 2013).

La simple entrega de la información vía electrónica, digitalizada u otro en términos automatizados, no garantiza que pueda ser reutilizada. Para ello, se requiere que sean entregados en ciertos formatos estructurados, abiertos y de uso común, con suficientes metadatos que garanticen su adecuada comprensión por

terceros, entre otras consideraciones técnicas. Por el contrario, la simple entrega de archivos en formatos Word, PDF, PNG u otros, no da la garantía antes señalada, es decir, puede ser directamente reutilizada.

Así, para garantizar la reutilización y obtener los beneficios económicos en favor del titular de los datos personales que se detallarán, es necesario reformular que la naturaleza del derecho a la autodeterminación informativa abarque un adecuado control sobre los datos personales automatizados tratados por terceros, es decir, que se permita reutilizarlos en el entorno digital, lo que supera el límite legislativo del derecho de acceso.

Prueba de ello es que, el 10 de junio de 2021, la Presidencia del Consejo de Ministros (PCM) solicitó al Congreso de la República, con carácter de urgencia y base legal en el artículo 105º de la Constitución, someter a consideración el Proyecto de Ley Nº 7870/2020-PE, Ley que crea la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales [Proyecto de Ley], cuya finalidad es brindar transparencia y acceso a la información pública[79], y fortalecer la protección de datos personales. Este busca incorporar el artículo 23-Aº (Derecho a la portabilidad de datos), dentro de la LPDP (2011) bajo la siguiente fórmula legal:

1. El titular del dato tiene derecho a recibir los datos personales sobre sí mismo, que haya facilitado a un responsable o titular del banco de datos, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable o titular del banco de datos personales cuando suceda lo siguiente:

a) El tratamiento esté basado en el consentimiento o en una relación contractual en la que el titular del dato es parte.
b) El tratamiento se ejerza mediante medios automatizados.

[79] Vía Decreto Legislativo Nº 1353, la Dirección General de Protección de Datos Personales se incorporó a la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, manteniéndose dentro del Ministerio de Justicia y Derechos Humanos.

2. Al ejercer su derecho a la portabilidad de los datos antes mencionados, el titular del dato tiene derecho a [que] sus datos se transmitan directamente de un responsable o titular del banco de datos a otro cuando sea técnicamente posible.
3. El derecho a la portabilidad no se aplica al tratamiento necesario para el cumplimiento de las competencias o funciones conferidas a las entidades públicas.

El fundamento expresado en su Exposición de Motivos (2021) es reforzar "el control de los datos personales que le conciernen a una persona natural" (p. 28) para que cuando "el tratamiento se realice por medios automatizados y sea técnicamente posible, el titular de los datos personales pueda solicitar al responsable del tratamiento o titular del banco de datos [los] transmita a otro responsable o titular de banco de datos" (p. 28). Se enfatiza lo siguiente:

> [N]o es ajeno al régimen peruano, pues en el sector de las telecomunicaciones se reconoce la portabilidad numérica, lo cual se traduce en el derecho de los usuarios de servicios de telecomunicaciones de conservar su número de teléfono, [aun] cuando cambie de empresa operadora de servicio móvil o fijo (p. 28).

La mencionada Exposición de Motivos (2021) también indica que el derecho a la portabilidad de los datos personales "se encuentra relacionado al derecho de acceso (…) ya que permite recibir los datos que sí mismo le haya dado al responsable del tratamiento o titular de banco de datos y poder transmitirlo a otro responsable o titular". Al respecto, la mayoría de la doctrina y la legislación extranjera consideran que el derecho a la portabilidad no es un derecho relacionado al derecho de acceso.

En su caso señalan que todos los derechos del titular de los datos personales estarían relacionados entre sí, ya que fueron concebidos para proteger el derecho a la autodeterminación informativa dentro del marco normativo de protección de los datos personales. En todo caso, debió sustentarse que este es un derecho que subyace al derecho de acceso. Por ello, no constituye *per se* un nuevo derecho,

pues la lógica detrás es simplemente una expresión o actualización del inminente fenómeno de digitalización frente al acceso de los datos personales y la necesidad de garantizar su reutilización ante tratamientos automatizados.

En la actualidad, esto implica que el derecho de acceso habría quedado parcialmente incompatible o inutilizable al querer reutilizarse o destinarse a otras finalidades. Esto tomando en cuenta que el tratamiento de los datos personales se da, principalmente, por medios automatizados y/o digitalizados. De aquí, nace la imperante necesidad de que sean portables y se les brinde importancia a las necesidades técnicas del formato proporcionado.

Si bien algunas autoridades, como la europea, optaron por la opción legislativa de incorporar dicho derecho, como uno nuevo e independiente, a efectos de fortalecer y promover su aplicación en el sector privado[80], no dejaron de reconocer que pertenece al existente derecho de acceso, con ciertas particularidades necesarias para su funcionamiento y que fueron agregadas por el legislador. Al respecto, Li (2018) cuenta que esta proximidad, entre ambos derechos, se refleja incluso en la historia legislativa, pues la Comisión Europea declaró, inicialmente, que el derecho a la portabilidad de datos personales sirve como condición previa y para mejorar aún más el acceso de las personas, aparece como un mecanismo para aclarar y mejorar el derecho de acceso.

Sin embargo, comenta que los dos derechos no son esencialmente idénticos, al menos no en la versión final del RGPDP (2016). En ese mismo sentido, el Grupo de Trabajo del Artículo 29 (2017) reconoce que el nuevo derecho a la portabilidad de datos personales está estrechamente relacionado con el derecho de acceso, pero se diferencia de él en muchos aspectos; complementa el derecho de acceso sobre todo al eliminar la restricción del formato de datos elegido por el responsable del tratamiento. Probablemente, dicha redacción haya inspirado

[80] Ello debido a que, como cuenta el Grupo de Trabajo del Artículo 29 (2017), dicho derecho requieremucho más que una simple incorporación legislativa. Necesita un despliegue técnico coordinado y consensuado en el mercado. En ese sentido, también trae considerables consecuencias en el mercado a favor de los agentes económicos.

rápidamente al proponente sin percatar otros contextos ponderados para su formulación.

Por el contrario, otras legislaciones, como el estado de California, en Estados Unidos, optaron por incorporar este requerimiento de emplear un formato portable cuando el derecho de acceso sea ejecutado por medios electrónicos de una manera distinta:

> (d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. (Civil Code. Division 3, Part 4, Title 1.81.5. California Consumer Privacy Act [CCPA] 2018, Art. 1798-100. 28 de junio de 2018, Estados Unidos de América)[81].

En tal legislación no se distingue, expresamente, entre uno u otro derecho, ya que, en la práctica, al momento de proporcionar electrónicamente los datos personales, debe garantizarse su reutilización. Por el contrario, se advierte prematuramente que, en la legislación europea y en el Proyecto de Ley (2021), la razón por la que se incorpora como un derecho nuevo y no como un requisito cuando el derecho de acceso sea proporcionado por vía digital, es porque se agregan, a su vez, varias excepciones o particularidades, que generan que su ámbito de aplicación sea más limitado. Esto no sucede en la opción legislativa adoptada en el Estado de California.

[81] Significa que una empresa que reciba una solicitud de consumidor constatable de un consumidor para acceder a información personal deberá tomar medidas de inmediato para divulgar y entregar, sin cargo al consumidor, la información personal requerida por esta sección. La información puede enviarse por correo o electrónicamente y, si se proporciona electrónicamente, la información deberá estar en un formato portátil y, en la medida en que sea técnicamente factible, de fácil uso que permita al consumidor transmitir esta información a otra entidad sin obstáculos.

Con todo, el Proyecto de Ley (2021) resulta preliminarmente positivo al poner sobre la mesa la discusión de incorporar una vía expresa para ejercer la portabilidad de los datos personales en entornos automatizados. A la fecha, para que un titular de datos personales pueda portar sus datos personales y/o compartirlos a otro responsable, se espera que los extraiga y cargue, cuando ello sea posible, en otro banco de datos personales, asumiendo la responsabilidad (o imposibilidad) cuando el formato y la subsecuente lectura de los datos descargados no sean compatibles o incompletos. Ellos son riesgos semánticos y sintácticos en la compatibilización que podrían abordarse legislativamente, si se determinara la obligación de proporcionar datos en un formato que sea reutilizable.

CAPÍTULO II: IMPLICANCIAS ECONÓMICAS Y TÉCNICAS DE LA PORTABILIDAD DE DATOS PERSONALES EN EL SECTOR DIGITAL

2.1 Consideraciones previas al acceso de los datos en el mercado digital

En los últimos años, tanto gobiernos como entidades internacionales han promovido distintas iniciativas para mejorar el acceso y el intercambio de datos en el sector público y privado. La OCDE (2019a) sostiene que se debe maximizar el acceso y el intercambio de datos entre los países[82] porque generan beneficios sociales y económicos (p. 15).

Así, a medida que más desarrollo se presenta en los mercados, los datos se consolidan como intrínsecos en las transacciones comerciales. Esto ha llevado a varios actores académicos y políticos, como señala Ciuriak (2018), a propugnar por la necesidad de que los datos fluyan libremente, incluso a niveltransfronterizo, como la quinta libertad de comercio, junto a la libertad de movermano de obra, capitales, bienes y servicios[83] (p. 6). Esta discusión, por ejemplo, se aborda en múltiples acuerdos comerciales, como el caso del, entrado envigencia, Acuerdo Transpacífico de Cooperación Económica (CPTPP) del que Perú y otros diez (10) países forman parte. Este acuerdo prohíbe, entre otros, la localización de datos y compromete a las partes al libre flujo de datos, a través de

---

82 Así, los estudios realizados por la OCDE (2019) estimaron que maximizar el acceso e intercambio de datos en sus países miembros y las economías asociadas, les generaría valor de entre el 0,1% y el 1,5% de su producto interno bruto (PIB), en el caso de los datos del sector público; y, entre el 1%y el 2,5% del PIB (algunos estudios concluyeron que incluso hasta el 4% del PIB), cuando tambiénse incluyan datos del sector privado. Por supuesto, la magnitud estimada de los efectos dependerá del alcance (contenido de los datos y los sector o sectores en los que se aplicará) y del grado de apertura de los datos que se implemente.

83 En estos esfuerzos, países como Estonia (incluso más que el resto de la Unión Europea) han llevado la delantera en la iniciativa. Para mayor información ver: https://e-estonia.com/free-movement-of-data-as-the-5th-fundamental-freedom-of-the-european-union/ y https://www.europarl.europa.eu/news/es/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom

las fronteras, aunque con tolerancia para las restricciones que puedan ser necesarias con el fin de lograr un objetivo legítimo de política pública.

La mencionada contextualización internacional permite entender el trasfondo de distintas políticas públicas destinadas a mejorar el acceso e intercambio de datos[84]. Así, la OCDE (2019a) resalta que, para alcanzar laapertura de datos[85], hay diferentes enfoques que giran en torno al acceso, intercambio y reutilización de datos por parte de los actores involucrados, y, con ello, la existencia o no de restricciones técnicas, legales u organizativas que los actores involucrados encontrarán (pp. 65-66).

Preliminarmente, la OCDE (2015) reconoce que no hay una única solución o enfoque adecuado para los desafíos que plantea el acceso e intercambio de datos. El enfoque más apropiado y el grado de apertura adecuado dependerán de los diferentes tipos de datos y los riesgos asociados con su reutilización, los diferentes actores y sus roles. Así, los datos que se anonimizan y agregan de manera efectiva, en principio, se deberían compartir de manera más abierta, pues encarnan menos riesgo a violaciones de la privacidad.

Los múltiples enfoques para mejorar el acceso e intercambio de datos han sido agrupados por la OCDE (2019a), en base a la doctrina y formulación de políticas públicas de gobiernos en el mundo, en torno a los datos abiertos, mercados de datos y portabilidad de datos.

El primer enfoque es denominado *Open Access*. Es el más utilizado para mejorar el acceso (apertura) a los datos (OCDE, 2015) y ha sido

[84] Con ello la OCDE (2019a), entre otros detalles, se refiere a aquellos mecanismos y enfoques destinados a maximizar los beneficios sociales y económicos de un uso más amplio y eficaz de losdatos, mientras que se aborden los riesgos y desafíos relacionados a dicho objetivo.

[85] La OCDE (2015) encuentra los siguientes grados de apertura: nivel 0 (data cerrada), acceso solo por el responsable del tratamiento; nivel 1 (discriminatorio), acceso solo por los titulares de los datos personales; nivel 2 (controlado), acceso solo para los miembros de una comunidad; y, nivel 3 (datos abiertos), acceso para el público (pp. 65-66).

satisfactoriamente empleado en el sector público. Los datos gubernamentales abiertos han sido promovidos por iniciativas, como *data.gov*, en Estados Unidos; *data.gov.uk*, en Reino Unido; *data.gov.fr*, en Francia; y, *data.go. jp*, en Japón[86]. Este ha supuesto, en gran medida, un acceso en igualdad de condiciones para la comunidad nacional e internacional o al menor costo posible (no superior al marginal de difusión)[87]. No obstante, para casos de datos confidenciales y datos personales no es atractivo, en tanto se espera que los datos abiertos se proporcionen de forma gratuita o al costo marginal de producción y difusión como máximo. Esto desincentiva la comercialización con los mismos y/o los servicios de valor añadido.

El segundo enfoque es denominado por la OCDE (2015) como acuerdos comerciales y mercados de datos. Está orientado al sector privado y surge debido a las oportunidades de comercializar datos patentados negociando acuerdos bilaterales para vender o licenciar datos. Sin embargo, los hechos demuestran que se requieren nuevos modelos comerciales que consideren suficientemente los riesgos e intereses de todas las partes involucradas[88]. La OCDE (2019a), basada

---

86 Para mayor información ver: Ubaldi, B. (2013), *Open government data: Towards empirical analysisof open government data initiatives*, OECD Working.

87 Esto ya ha sido señalado desde años anteriores. Para mayor información ver: https://legalinstruments.oecd.org/public/doc/122/122.en.pdf

88 Un ejemplo fue el escándalo de la empresa Cambridge Analytica que hacía minería de datos, análisisy corretaje que permitió acceder a datos personales de más de 50 millones de personas, aunque solo unas 270 000 personas "habrían dado su consentimiento para que se recopilaran sus datos" (Granville, 2018; Cadwalladr y Graham-Harrison, 2018). El escándalo empezó cuando se constató que se encontraba brindando masivamente servicios en campañas políticas, mediante difusión de noticias y demás contenido político, incluso con *hate speech* [mensajes de odio] y *fake news* [noticias falsas] de la competencia en las sesiones de inicio de usuarios de Facebook y otras cuentas vinculadas para influir en las decisiones de los votantes en favor del partido político y/o candidato contratado.

Así, se alega que influyó ilegalmente en la campaña presidencial de Estados Unidos, en 2016, a favor del presidente ganador (Donald Trump), en el referendo de separación de Inglaterra del resto de la Unión Europea (Brexit 2016), en varias campañas electorales de África, Sudamérica y otras campañas electorales alrededor del mundo. Para mayor información ver: https://www.bbc.com/mundo/noticias-43472797. Finalmente, en sede nacional, nuestra autoridad emitió una nota de prensa, el 24 de mayo de 2018, solicitando información a Facebook sobre el caso

en su estudio de 2015, ha clasificado las siguientes modalidades contractuales en el mercado digital en torno a los datos:

- *Freemium*: acrónimo de gratis y *premium* en inglés. Los productos se proporcionan de forma gratuita, pero cobrando dinero por funciones adicionales *premium*, a menudo patentadas. Este suele combinarse con el modelo de ingresos basado en publicidad. Aquí, el producto gratuito se ofrece con publicidad y el premium no[89].

- Publicidad: se utiliza con mayor frecuencia para ofertas de empresa a consumidor (B2C). Los productos se ofrecen de forma gratuita o con un descuento a los usuarios a cambio de la visualización obligatoria de anuncios pagados. Es utilizado en mercados multilaterales, donde un servicio se proporciona de forma gratuita o a un precio bajo, en un lado del mercado (usuarios del sitio web consumidores), y se subsidia con ingresos de otros lados del mercado (usuarios del sitio web vendedores). Un caso son los anuncios pagados en la plataforma de videos de YouTube[90].

- Suscripción: son los más utilizados en el ecosistema de datos para las ofertas negocio a negocio (B2B), en particular. Estos incluyen pagos regulares (diarios, mensuales o anuales) para acceder a contenido digital y, a menudo, se combina con el modelo de ingresos *freemium*.

- Tarifas de uso: son el segundo modelo de ingresos más utilizado y destacado para las ofertas B2B. Generalmente, se cobran a los clientes por el uso real del servicio en línea u ofertas que se brindan, como el almacenamiento en

---

Cambridge Analytica, a efectos de saber si ciudadanos peruanos también se vieron vulnerados. Para mayor información ver: https://www.gob.pe/institucion/minjus/noticias/4050-autoridad-de-proteccion-de-datos-personales-del-minjusdh-solicita-informacion-a-facebook-sobre-caso-cambridge-analytica

89 Un ejemplo es el servicio gratuito de Spotify versus su servicio *premium* (https://www.spotify.com/pe/premium/) y el servicio gratuito de Rappi versus su servicio RappiPrime (https://www.rappi.com.pe/prime)

90 Para mayor información ver: https://www.youtube.com/intl/es-419/ads/

la nube. Ejemplo de esto son los servicios conocidos como *Dropbox*, *Google Cloud Storage*, *Microsoft One Drive*, *IBM Cloud Storage*, *MediaFire*, entre otros.

- Venta de bienes (incluido contenido digital): considera los modelos de ingresos de pago por descarga, datos y contenido digital como música y videos[91]. Prueba de ello, son las innumerables plataformas de bancos de datos que se dedican a la venta de imágenes en línea y se pagan por descarga, como *Shutterstock* y *iStockPhoto.*

- Venta de servicios: incluye la prestación de servicios B2B los servicios prestados por intermediarios (como alojamiento web o *web hosting*) y el procesamiento de pagos. Por tanto, se superpone con los modelos de ingresos que se basan en suscripciones y tarifas de uso que, a menudo, se utilizan para los contratos de servicios de tecnologías de la información.

- Licencias: contrato que regula los términos y condiciones entre un proveedor de software y un tercero para su uso, distribución, omodificación. Existen varias modalidades en el mercado. Un ejemplo seríauna empresa adquieriendo herramientas para la gestión de sus bases de datos u otras soluciones en la nube de Oracle, vía licenciamiento[92].

- Tarifas de comisión: empleadas, sobre todo entre empresas y consumidores (B2C). Normalmente, ese cálculo de la tarifa se realiza gracias a intermediarios que utilizan el análisis de datos para ajustar mejor la oferta y demanda. Los pagos se calculan sobre un porcentaje del precio de los productos suministrados y solo se obtendrán cuando coincidan satisfactoriamente la oferta y demanda. Un ejemplo de esto son las empresas de taxi por aplicativo o intermediadores de servicios digitales, como Uber, Cabify, Taxibeat, entre otros.

---

91 *Shutterstock* (https://www.shutterstock.com/es/g/stockfilm/video?rid=2700319) y *iStockPhoto* (https://www.istockphoto.com/es).

92 Para mayor información ver: https://www.oracle.com/es/cloud/solutions/

El tercer enfoque, que es en el que se basará esta investigación, es la portabilidad de datos, considerado prometedor por varias instituciones como la *Productivity Commission* [Comisión de la Productividad del Gobierno de Australia (2017)[93] y la OCDE (2019a), pues promueve la reutilización intersectorial de datos al tiempo que fortalecen los derechos de control de las personas sobre sus datos personales y las empresas (sobre todo de las pequeñas y medianas). Así, la OCDE (2019a) reitera que la portabilidad de datos proporciona un acceso restringido que permite a los responsables del tratamiento y titulares del banco de datos proporcionar datos de sus clientes en un formato estructurado legible por máquina de uso común, ya sea directamente al cliente o a un tercero (p. 151).

Otros ejemplos o iniciativas de portabilidad de datos que destacan son las iniciativas *My Data* del gobierno de Estados Unidos (2010)[94] y *Midata portability*

[93] En el caso de Australia, se adoptó la siguiente estrategia: la Comisión de Competencia y Consumidores de Australia (ACCC) y la Oficina de la Comisión de Información de Australia (OAIC) anunciaron conjuntamente las "Competition and Consumer (Consumer Data Right) Rules"(2019) para ayudar a los consumidores y participantes a comprender el enfoque a adoptarse, en donde señalaron que los reguladores adoptarían, entre otras medidas:

> The data is disclosed to the person who made the request, in machine-readable form and in accordance with the data standards. A data holder must not impose conditions, restrictions or limitations of any kind on the use of the disclosed data (…) [los datos se comunican a la persona que hizo la solicitud, en forma legible por máquina y de acuerdo con los estándares de datos. Un titular de datos no debe imponer condiciones, restricciones o limitaciones de ningún tipo sobre el uso de los datos divulgados]. (numeral 2.1. Parte 2, Competition and Consumer [Consumer Data Right] Rules, 2019).

A la fecha, el régimen de Consumer Data Right se está implementando, progresivamente, en diferentes sectores de la economía, comenzando con el sector bancario y extendiéndose a la energía y las telecomunicaciones. Se está discutiendo la formulación de la "version 1.5.1 of the Consumer Data Standards (CDS)", aplicable a transferencias normas técnicas para el intercambio de datos de los consumidores, accesible en https://treasury.gov.au/consultation/c2021-168954. Para mayor información ver: https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-rules-banking

[94] Para mayores detalles sobre su funcionamiento y todas las demás subiniciativas y áreas en las que se implementaron. Para mayor información ver:

initiative del Reino Unido (2011)[95], las mencionadas como el derecho a la portabilidad de datos reconocido en el artículo 20° del RGPDP (2016) de la Unión Europea, y la legislación transversalmente implementada sobre el *Consumer Data Right*, en Australia.

Sin embargo, la OCDE (2019a) advierte que las iniciativas de portabilidad de datos vigentes varían significativamente en su naturaleza, alcance y aplicabilidad:

- Kokott y Sobotta señalan que la portabilidad de datos es concebida como medio para lograr la autodeterminación informativa: el régimen de protección de datos en la Unión Europea se sustenta, en parte, en el objetivo de proporcionar a las personas un mayor control sobre sus datos personales (como se cita en OCDE, 2019a). Por ello, solo los datos personales están dentro del alcance del RGPDP (2016) y no aplica a ningún dato que sea anónimo.

- La portabilidad de datos concebido medio para aumentar la competencia y la elección: entre proveedores de bienes y servicios digitales como, por ejemplo, entre proveedores de servicios de las redes sociales y en otros mercados analógicos como de servicios públicos (electricidad, agua, gas natural, etc.). La Unión Europea e Inglaterra alegan que la portabilidad de los datos puede mejorar la competencia, al reducir las asimetrías de información entre las personas, y los proveedores de bienes y servicios; limitar los costos de cambio para las personas; y, al disminuir potencialmente las barreras de entrada al mercado.

https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access

95 Para mayor información ver:

- https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment
- https://www.nationwide.co.uk/support/support-articles/manage-your-account/midata

- La portabilidad de los datos como medio para fomentar los mercados sobre nuevos productos en la Unión Europea e Inglaterra, al actuar como un estímulo para la expansión, innovación, y creación de nuevos productos y servicios[96].

- La portabilidad de datos como medio para facilitar los flujos de datos: un ejemplo de esto es el análisis de la Comisión Europea (2017) contenido en la "Comunicación de la Comisión al Parlamento Europeo, al Consejo, Comité Económico y Social Europeo, y Comité de las Regiones para la Construcción De Una Economía De Los Datos Europea". Esta tiene el objetivo de dialogar con las partes interesadas la futura regulación y promocionar temas como la libre circulación de datos, el acceso y la transferencia de los datos generados por máquinas, la responsabilidad y la seguridad en el contexto de las tecnologías emergentes, la portabilidad de los datos no personales, la interoperabilidad y demás normas asociadas.

Para la OCDE (2019a), todavía se está por determinar en qué medida la portabilidad de datos puede, verdaderamente, empoderar a los titulares de datos personales y fomentar la competencia e innovación. Las estimaciones sobre los costos y beneficios asociados, concretamente a la portabilidad de datos, aún son escasas. Sin embargo, podrían tener efectos económicos positivos generales en el mercado al reducir los costos de cambio ante las limitaciones existentes al traslado entre aplicaciones, que actúan una barrera para evitarlo. Ello se aprecia al cambiar de sistemas operativos en teléfonos inteligentes (de iOS de Apple al sistema

[96] Según la evaluación de impacto de Midata, el Reino Unido señala que el programa se implementó considerando que la publicación de datos de transacciones estimularía la innovación y la expansión de distintos servicios web como los Comparison Shopping Engines or Websites [motores o sitios web de comparación de precios] (Departamento de Innovación y Habilidades Empresariales (como se cita en OCDE, 2019a). También, destacó el fomento de otros posibles servicios derivados de su uso. Así, un minorista de comestibles finlandés líder se asoció con un tercero para informar a sus clientes del contenido nutricional de su canasta de compras basándose en datos agregados a través de tarjetas de fidelización. De tal manera, como señala el Departamento de Innovación y Habilidades Empresariales del Reino Unido se proporcionó una "herramienta de gestión del peso y la dieta en tiempo real para individuos y familias" (como se cita en OCDE, 2019a, p. 157).

operativo de Android) o en la portabilidad de números móviles en países en que todavía no es posible.

Habiéndose determinado que la portabilidad es un enfoque adoptado para mejorar el acceso, el intercambio y la reutilización de datos en el sector privado y el entorno digital, es necesario aterrizar definiciones asociadas a la portabilidad de datos personales para continuar con las implicancias económicas, técnicas y legales de incorporar dicha posibilidad como derecho del titular de los datos personales en la normativa peruana, así como prever qué condiciones y limitaciones deberían aplicarse.

2.2 ¿Qué es la portabilidad?

Según el Diccionario de la Real Academia Española [DRAE], la portabilidad es la cualidad de portable, asociada al verbo portar que la DRAE también define como "tener algo consigo o sobre sí"[97] y "llevar, conducir algo de una parte a otra".

Así, desde la perspectiva técnica, la (ISO/IEC 25000:2014) define a la portabilidad como la "[c]apacidad del producto o componente de ser transferido de forma efectiva y eficiente de un entorno *hardware*, *software*, operacional o de utilización a otro". A su vez, se indica que requiere de ciertas sub características como la adaptabilidad, que es ser adaptado de forma efectiva y eficiente a diferentes entornos determinados de *hardware*, *software*, operacionales o de uso; capacidad para ser instalado, y/o desinstalar de forma exitosa en un determinado entorno; y, capacidad para ser reemplazado, es decir, ser utilizado en lugar de otro producto software determinado con el mismo propósito y en el mismo entorno.

[97] Esta definición resulta curiosa, pues el verbo "tener" se puede asociar a la extendida idea de que el derecho a la portabilidad de datos intenta incorporar atributos similares del régimen de propiedad a los datos personales para permitirle participar en los beneficios económicos del tratamiento de sus datos personales. Lo anterior, podría deberse a los intentos realizados en torno a la viabilidad de un régimen "similar" al de propiedad, que otorgue mayor control frente a terceros. Esta idea será más discutida en la sección posterior destinada al aspecto económico.

La portabilidad de datos está también definida en el numeral 3.2.21 de la (ISO/IEC 17788:2014), el cual la identifica como la capacidad para transferir datos fácilmente de un sistema a otro sin necesidad de volver a ingresar datos. Lo esencial en la portabilidad es la facilidad de mover datos entre un sistema de origen al de destino. No se requiere que los formatos de origen y destinocoincidan, pero la transformación entre ellos debe ser factible con herramientas que estén comúnmente disponibles. Finalmente, se advierte que un proceso de imprimir los datos y volver a introducirlos a un sistema de destino no califica como portabilidad.

De igual manera, la portabilidad es un término asociado a la interoperabilidad, definida como la capacidad de dos o más sistemas o aplicaciones para intercambiar información y utilizar mutuamente la que se ha intercambiado (ISO/IEC 17788:2014, 3.1.5). Esto implica la posibilidad de que, dentro de entornos (sistemas o aplicaciones), se porte información y, posteriormente, se use mutuamente.

Sobre esta vinculación de conceptos, Gal y Rubinfeld (2020) indican que la portabilidad de datos es la capacidad de transferirlos sin afectar su contenido y la interoperabilidad, y de integrar dos o más conjuntos de datos. Ambos factores afectan el uso de los datos y, en consecuencia, el costo en cualquier tratamiento de ellos, independientemente del sector de la industria. Por ello, dicha portabilidad puede facilitar más (cantidad) y mejores (calidad) intercambios de datos, permitiendo que más entidades los utilicen.

Por su lado, la interoperabilidad de datos puede crear sinergias entre ellos, es decir, combinaciones de datos de diferentes fuentes para mejorar el conocimiento a extraer. Un ejemplo es el funcionamiento de una ciudad inteligente: los datos de diversas fuentes (semáforo, transporte público, sensor de contaminación, informes policiales, etc.) deben integrarse para permitir un trabajo sincronizado y eficiente.

Por ende, no es sorprendente que las barreras de la portabilidad e interoperabilidad se hayan identificado como bloques importantes para el funcionamiento eficiente en las economías intensivas en datos. Esto ha sido

abordado dentro de la estrategia de la Unión Europea para implementar un mercado único de datos[98], que, entre otros objetivos, impulse la interoperabilidad y portabilidad dinámica de los datos en tiempo real para las personas y empresas con respecto a datos personales y no personales. Así, Varian reconoce que la construcción de esta canalización de datos es, a menudo, la parte más laboriosa y costosa de la construcción de una infraestructura de datos, ya que diferentes empresas, a menudo, tienen sistemas heredados idiosincrásicos[99] que son difíciles de interconectar (como se cita en Graef, Tombal y de Streel, 2019).

Según Crémer, de Montjoye y Schweitzer (2019) existen tres tipos de interoperabilidad: de protocolos, que es la capacidad de dos servicios o productos para interconectarse, técnicamente, entre sí, y los emplean en políticas de competencia en la legislación europea; de los datos, que es equivalente a la portabilidad de los datos, pero con un acceso continuo y, potencialmente, en tiempo real a los datos personales o de sus usuarios[100]; y, de protocolo completo, que se refiere a estándares que permiten que los servicios sustitutos interoperen entre ellos, como los sistemas de mensajería.

En sede nacional, estos conceptos han sido abordados normativamente por el Decreto Legislativo Nº 1412, Ley de Gobierno Digital, que prevé en su artículo 26° que la interoperabilidad[101] es una capacidad de interactuar entre "las

---

98 Para más información ver: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data- 19feb2020_en.pdf

99 La DRAE (s.f.) define idiosincrasia como aquellos "rasgos, temperamento, carácter, etc., distintivosy propios de un individuo o de una colectividad". En este caso, se asocia a los de una empresa en particular para aludir a sus procesos organizativos internos y demás dinámicas propias.

100 A la fecha, los mecanismos de interoperabilidad de datos existentes, generalmente, se basan en API privilegiadas que brindan a un servicio los medios para acceder a los datos de sus usuarios a través de la API de otro servicio cuando los usuarios han dado autorización para esta transferencia de datos.

101 Las materias de gobierno digital comprenden los siguientes elementos:

> [t]ecnologías digitales, identidad digital, interoperabilidad, servicios digitales, datos, seguridad digital y arquitectura digital, los cuales se relacionan entre sí con la finalidad de mejorar la prestación de servicios centrados en los ciudadanos, la gestión interna de las entidades de la Administración Pública y la relación entre estas en la prestación interadministrativa de servicios públicos de manera segura para fortalecer la confianza y

organizaciones diversas y dispares para alcanzar objetivos que hayan acordado conjuntamente, recurriendo a la puesta en común de información y conocimientos, a través de los procesos y el intercambio de datos entre sus respectivos sistemas de información".

Dicha norma considera un Marco de Interoperabilidad del Estado Peruano[102] que, conforme a su artículo 27°, está constituido por políticas, lineamientos, especificaciones, estándares e infraestructura de tecnologías digitales, que permiten, de manera efectiva, la colaboración entre entidades públicas para el intercambio de información y conocimiento, el ejercicio de sus funciones en el ámbito de sus competencias y la prestación de servicios digitales interadministrativos de valor para el ciudadano en canales digitales. En el artículo 28°, se detallan los siguientes niveles para su gestión:

- Organizacional: se enfoca en el alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades públicas para intercambiar datos e información para el ejercicio de sus funciones.
- Semántico: relativo al uso de los datos y a la información de una entidad, garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada puedan ser entendidos por cualquier aplicación de otra entidad pública. Por ello, deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.
- Técnico: abocado a aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información. También, define los protocolos de comunicación y seguridad

satisfacer las necesidades de los ciudadanos y personas en general en el entorno digital, orientado a la transformación digital del Estado [subrayado añadido] (artículo 2.2º, Decreto Supremo N°029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, 2021).

[102] Para mayor información consultar los artículos 82° a 93° del Decreto Supremo N°029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. Además, revisar la Plataforma Nacional de Interoperabilidad: https://www.gob.pe/741-plataforma-de-interoperabilidad-del-estado

necesarios. Es ejecutado por personal de las oficinas de informática de las entidades públicas, de acuerdo a los estándares definidos por el ente rector.

- Legal: busca la adecuada observancia de la legislación y lineamientos técnicos para facilitar el intercambio de datos e información entre las entidades públicas y el tratamiento de la información intercambiada.

Conforme a las experiencias o consideraciones extranjeras y nacionales desde el sector público, algunas observaciones preliminares pueden esbozarse en torno a la portabilidad de datos: implica la facilidad de transferencia sin necesidad de volver a ingresar la data y su posterior posibilidad de reutilización; la necesidad de formatos o estándares comunes o, al menos, compatibles; su indiscutible asociación al tratamiento automatizado de datos personales; su vinculación a la interoperabilidad; la necesidad de generar consensos y colaboración entre agentes del mercado para poder materializar la portabilidad de datos; e, implicancias económicas que deben ser estudiadas. La OCDE (2019a) concuerda con que existen diversas implicancias e impactos económicos y técnicos en el mercado digital que deben analizarse para determinar los costos y beneficios de materializar la portabilidad de datos de carácter personal.

2.3 Implicancias económicas de la portabilidad de datos en el sector digital

A efectos de determinar cuáles serían las implicancias económicas de la portabilidad de datos personales en el sector digital, se iniciará analizando las particularidades de este sector en base a la experiencia nacional e internacional.

2.3.1 Particularidades del mercado digital en sede nacional

A inicios de 2020, la Secretaría de Gobierno y Transformación Digital [SGTD] de la Presidencia del Consejo de Ministros, en la Agenda Digital del Bicentenario[103], en base a cifras del Ministerio de la Producción del año 2016,

[103] Dos conceptos claves que se deben tener en cuenta, de acuerdo a la SGTD (2020) son los siguientes:"la digitalización se da cuando se adoptan soluciones digitales dentro de los procesos habituales deuna empresa o entidad estatal" (p.2) y la transformación digital "[e] un proceso que responde a las necesidades de supervivencia de las oganizaciones, generando una reinvención, una modificación en la estrategia o en el modelo de negocio" (p.2).

reportó que, si bien el 99% de las empresas peruanas eran micro y pequeñas empresas, solo el 12% compraba por Internet, bajo cualquier modalidad. Asimismo, el 7% de las empresas vendía por Internet y se debía a que solo el 29% de la población nacional estaba bancarizada.

Este panorama ha sufrido drásticos cambios tras la pandemia de la COVID-19. En el 2021, la Cámara Peruana de Comercio Electrónico [CAPECE] ha advertido que, dicho año, es el Año 1D.C. (Después de la COVID-19)[104]. Con ello, el enorme impacto que la crisis sanitaria causó en el país[105], al volver mandatorio el distanciamiento y el aislamiento social, y otros factores como el desempleo generado por la paralización de casi todos los sectores tradicionales de la economía con excepción de bienes de primera necesidad y otros productos de hogar, volcaron una desesperada atención al sector digital sin precedentes.

CAPECE (2021) advierte que las micro, pequeñas y medianas empresas en medio de la crisis sanitaria han sido claves para la reactivación económica y foco para las estrategias de digitalización del mercado peruano y de las iniciativas del Gobierno Digital en el Perú[106]. También, indica que el impacto de la COVID-19

[104] Según el Ranking de Competitividad Digital Mundial, al 2020, Perú ingresó al puesto 55 en competitividad digital. El 2019, se encontró en el puesto 61.

[105] CAPECE (2021) advierte que la pandemia de la COVID-19 ha golpeado a muchas economías, especialmente, las latinoamericanas; sin embargo, Perú ha sido el segundo país más afectado económicamente. Incluso, algunos estiman que es la tercera a nivel mundial. A ello se suma la crisis política y social por las malas gestiones del gobierno para atender la crisis sanitaria, los múltiples escándalos políticos que generaron el cierre del congreso, los cambios de gobiernos y los resultados electorales que han generado todavía más polarización y escepticismo en la sociedad peruana. Para mayor información ver: https://www.efe.com/efe/america/politica/peru-un-ano-de-tormenta-perfecta-pandemia-recesion-y-feroz-crisis-politica/20000035-4481534.

[106] La propia SGTD (2021) indica que se viene trabajando un gran avance en el proceso de transformación digital, despliegue de las tecnologías de la información y comunicaciones en favor de los ciudadanos a nivel nacional. Para ello, se ha emitido un marco normativo acorde con la transformación digital, en el Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital, y el Decreto de Urgencia Nº 007-2020, que aprueba el marco de confianzadigital y dispone medidas para su fortalecimiento. Las nuevas necesidades, generadas durante la pandemia por COVID-19, también ayudaron a acelerar este proceso, hallándose soluciones

ha acelerado avances del comercio electrónico que estaban previstos para 5 años, en solo 3 meses, entrando a categorías en las que no tenía participación. Incluso, el *e-commerce* ha sufrido cambios en los hábitos de consumo. Se afirma que, durante el 2019, los consumos más recurrentes fueron los vuelos y el turismo, pero tuvieron una contracción del 75%, el 2021. CAPECE (2021) indica que este espacio fue tomado por el *e-commerce retail*, que aumentó un 250%, y por los bienes digitales y pago de servicios[107]. Por ello, según INEI, a la fecha la industria del comercio electrónico en el país tiene un tamaño de mercado de USD 6 millones de dólares y el número de empresas que ingresaron al *e-commerce* aumentó en 400%, en el 2020[108] (como se cita en CAPECE, 2020).

En medio de este panorama, CAPECE (2021) advierte que los hábitos del consumidor habrían sido reseteados, pues "existe un marcado incremento en el consumo de contenidos digitales de alto valor, rechazo a contenidos vacíos, y conexión con marcas que demuestran tener un propósito sincero, y están haciendo algo para impulsar la economía" (p. 5).

No obstante, CAPECE (2021) indica que el país debió enfrentarse a otra realidad difícil: "el bajo nivel de digitalización de nuestro mercado" (p. 6). En ese

empáticas a las necesidades ciudadanas sencillas y evitando contacto físico: "[e]ste esfuerzo se evidencia en los indicadores en materia de Gobernanza digital, Innovación digital, Seguridad Digital, Confianza digital, Gobierno de datos, Interoperabilidad en el Estado y Gestión documental digital" (SGTD, 2021). Para mayor información ver: https://indicadores.digital.gob.pe/

Adicionalmente, existen múltiples estrategias que han sido llevadas a cabo comprendiendo a entidades públicas, empresas del sector privado y la academia, como las Estrategias Nacionales, sobre IA, Gobierno de Datos, Innovación Digital, Seguridad y Confianza Digital y Talento Digital.

[107] CAPECE (2021) advierte que los bienes digitales, generalmente, están vinculados con "el consumode productos y servicios de app, juegos en línea, descargas digitales, *streaming*, *e-learning, app delivery*, taxi por aplicativo, *software*" (p.9). Estos suelen ser pagos transfronterizos. Los servicios digitales comprenden "los pagos de impuestos al gobierno y servicios públicos (luz, agua, gas, educación, entre otros)" (CAPECE, 2021, p. 9).

[108] CAPECE (2021) también indica que el 36.1% de la población es compradora en línea, pues el 76.2%de los hogares cuentan con internet.

sentido, CAPECE (2021) describe la realidad del comercio electrónico[109] económica y política en pandemia de la siguiente manera (p. 12):

- Restricciones en el comercio electrónico: la logística, incluyendo el *delivery*, por compras realizadas en *e-commerce*, fue suspendida casi en su totalidad hasta mayo de 2020, salvo para productos de primera necesidad. Esto agravó la recesión.

- Restricciones territoriales: para frenar la expansión de la COVID-19, las entregas vía comercio electrónico, inicialmente, solo funcionaron en sus respectivas regiones, lo que generó que las ventas *online*, en provincias del Perú, no se desarrollasen como en la capital, durante el primer semestre de 2020.

- Ola de reclamos: aumentó la desconfianza sobre las compras vía *online*, debido al incumplimiento de los proveedores.

- Informalidad digital: en los mercados tradicionales, las empresas presentaban altos índices de informalidad. Lo anterior se ha reflejado en el comercio digital, el cual no está bien organizado, empezando por "sus redes sociales, donde no hay términos y condicionales, ni tampoco libro de reclamaciones y donde el *delivery* y la transacción no está garantizada" (CAPECE, 2021, p.12).

[109] CAPECE (2021) indica que, para definir el comercio electrónico, la Organización Mundial de Comercio [OMC] sostiene que implica a toda producción, distribución, mercadeo, venta o entrega de bienes y servicios por cualquier medio electrónico a empresas, hogares, individuos, gobiernos u otras organizaciones públicas o privadas. Es decir, el comercio electrónico "no es exclusivo de quienes tienen una tienda online sofisticada, las MYPES [microempresas] nos ayudaron a entender el concepto al dar el salto al canal online, apoyados en marketplaces, redes sociales, e incluso ayudándose del aplicativo móvil de WhatsApp" (CAPECE, 2021, p.8.), es decir, cualquier medio digital es válido.

Este panorama llevó a muchas entidades a intervenir, por ejemplo, la Dirección de Fiscalización e Instrucción (DFI) de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (DGTAIPD), "no solo incrementó las fiscalizaciones, cantidad de resoluciones e imposición de multas; sino que también potenció, como consecuencia de la pandemia, las modalidades de supervisión y fiscalización, virtualizando aún más los servicios administrativos" (Bolaños, 2021). Así, entre las múltiples fiscalizaciones remotas a los sitios web durante la pandemia, resalta la creciente preocupación e interés de dicha autoridad por el uso de *cookies* en sitios web y aplicativos sin informar ni obtener adecuadamente el consentimiento de los titulares de los datos personales, conforme al artículo 18º de la LPDP (2011)[110].

Por su parte, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [INDECOPI], emitió, el 5 de abril de 2021, el Documento de Trabajo Institucional "Propuestas para la protección del consumidor en el comercio electrónico y la seguridad de productos"[111]. Este pretendió abordar aspectos no previstos para la contratación por medios digitales, tales como la introducción del derecho de arrepentimiento; la garantía de la seguridad de los productos para evitar riesgos o peligros injustificados al comprar por un canal digital; la regulación de la figura de los intermediarios de servicios digitales a efectos de que también sean considerados como proveedores de servicios bajo ciertos supuestos, como cuando fijen el precio del producto o servicio ofrecido; el establecimiento el deber de información veraz, clara y completa (reforzando la figura ya existente en la normativa vigente); entre otras propuestas.

Sin embargo, dicha iniciativa deberá ser aprobada legislativamente para que pueda entrar en vigencia. A la fecha, no hay certeza sobre si su implementación será en un corto, mediano o incierto plazo. Además, pese a que las modificaciones

110 Para mayor información ver: https://elperuano.pe/noticia/114743-juridica-las-cookies-en-sitios-web

111 Para mayor información ver: https://www.gob.pe/institucion/indecopi/noticias/311694-el-indecopi-prepara-una-propuesta-normativa-para-el-comercio-electronico-con-el-fin-de-fortalecer-la-proteccion-del-consumidor-digital

propuestas tuvieron como motivo la intensificación del uso del comercio electrónico en la pandemia, se sustentan en las observaciones del año 2019, en el "Examen voluntario entre homólogos del derecho y la política de protección del consumidor del Perú"[112]. Tal examen fue realizado para identificar, a través de una evaluación externa e independiente, las mejoras pendientes al marco jurídico e institucional para la protección de los consumidores.

Algunas de las recomendaciones expresas por parte de la Conferencia de las Naciones Unidas sobre el Comercio y Desarrollo [UNCTAD] a la PCM, INDECOPI y al resto de entidades del Sistema Nacional Integrado de Protección del Consumidor fueron "[el] examinar la legislación para, en su caso, adaptarla a las necesidades del comercio electrónico a la luz de las Directrices de las Naciones Unidas para la Protección del Consumidor y las Recomendaciones de la OCDE" (p. 60) e incluir "como eje principal de acción, la protección del consumidor en el comercio electrónico y, a su vez, incluir la protección del consumidor en las políticas nacionales de más alto rango, como el Plan Bicentenario sobre gestión digital" (pp. 60-61).

Estos son algunos de las múltiples acciones y medidas gubernamentales como respuesta al inminente cambio en la economía peruana que tomaron fuerza durante la pandemia. Ante ello, nacen las siguientes cuestiones: ¿qué riesgos y cambios trae digitalizar la economía? ¿Qué particularidades deben ser advertidas por las autoridades y ciudadanos peruanos? ¿Tienen razón los organismos internacionales al recomendar la adaptación y el fortalecimiento de nuestros marcos legislativos al sector digital o basta con lo que ya existe, sobre todo, en el sector privado, pues se corre el riesgo de desincentivar la digitalización e innovación en un sector en desarrollo?

[112] Para mayor información ver: https://www.gob.pe/institucion/indecopi/noticias/309305-naciones-unidas-evalua-la-politica-peruana-de-proteccion-del-consumidor-y-plantea-recomendaciones-de-mejora

2.3.2 Particularidades del mercado digital en sede global

Los mercados digitales presentan ciertas particularidades frente a los mercados tradicionales. Estos realizan el intercambio de bienes o servicios prescindiendo del uso de la tecnología. En uno digital, el comercio se realiza sobre bienes o servicios, tanto físicos como digitales, siendo imprescindible la tecnología para el comercio.

Además, en dicho entorno las empresas tecnológicas, por lo general, son titulares de plataformas digitales, mediante las cuales operan. Estas plataformas son definidas, por la Comisión Europea, como "empresas que operan en mercados de dos o múltiples partes, que utilizan Internet para facilitar las interacciones entre dos o más grupos de usuarios distintos pero interdependientes, a fin de crear valor al menos para uno de esos grupos" (como se cita en UNCTAD, 2019, p. 3). Estas engloban servicios y actividades como mercados en línea, redes sociales, motores de búsqueda, sistemas de pago, entre otros. Este mercado también posee ciertas características clave como las siguientes:

- Barreras de entrada: se presume que, al ser los costos de entrada bajos, no existirían mayores barreras de entrada al mercado. No obstante, si bien algunas de estas, como los costos de capital, infraestructura, etc., son menores que en mercados físicos, hay otras a ser consideradas.

  Los datos, en sí mismos, pueden constituir una barrera de entrada a los mercados digitales, pues las empresas dominantes podrán recopilar grandes cantidades de datos personales y utilizarlos para mejorar su oferta de productos y la monetización de sus servicios, mediante el desarrollo de publicidad dirigida. En ausencia de aquellos, los nuevos participantes pueden tener dificultades para competir, por ejemplo, dentro del mercado de la publicidad digital (UNCTAD, 2019)[113].

[113] Así, UNCTAD (2019) indica que es muy difícil que una plataforma entrante al mercado alcance tráfico en línea: "las empresas emergentes enseguida deben afrontar la presión de la competencia ypueden acabar siendo compradas por las plataformas dominantes" (p. 4). Desde su fundación en

Además, “las plataformas dominantes también se han expandido abarcando actividades conexas, con el fin de tener acceso a más datos” (UNCTAD, 2019, p. 5). Las plataformas digitales dan prioridad, a corto o medio plazo, al crecimiento sobre los beneficios, es decir, a conseguir el máximo número de usuarios y no de beneficios. Las plataformas dominantes pueden permitirse esa estrategia comercial, dado que los inversores les otorgan margen para soportar pérdidas. Por ejemplo, Kahn menciona que los inversores permitieron que *Amazon* creciera sin exigirle que presentara beneficios, por lo que amplió su actividad y afianzó su dominio como mercado de comercio electrónico (como se cita en UNCTAD, 2019).

Finalmente, los costos de cambio son relevantes en tanto que “estudios de las tendencias del comportamiento indican que cambiar de plataforma conlleva un costo cognitivo, ya que requiere tiempo, esfuerzo, energía y concentración y reflexión” (UNCTAD, 2019, p. 5). Esto refuerza el dominio y el poder de mercado de la plataforma dominante, aunque no siempre las plataformas dominantes tienen competidores. Por ello, los consumidores tienen escasas opciones para cambiar y poco control sobre el tratamiento de sus datos.

- Efectos de red: estos implican mayor utilidad en el uso de un bien o servicio, mientras más consumidores lo usan (Laserre y Mundt, 2017, p. 95).

  Si los agentes beneficiados con dicha utilidad son del mismo tipo, se le denomina un efecto de red directo. Aquí, un ejemplo serían los usuarios de una red social o teléfono que pueden comunicarse con más personas. Si, gracias a una mayor participación de agentes de un tipo, se aumenta el valor de la plataforma para agentes de otro tipo, se le denominará un efecto de red

1998, Google ha adquirido, al día de hoy, 22 de junio de 2021, 225 entidades mercantiles por al menos diecinueve (19) billones de dólares de los Estados Unidos. Para mayor información ver: https://acquiredby.co/google-acquisitions/

indirecto[114]. Esto ocurre cuando dos o más lados distintos de un mercado se benefician como resultado de la interacción en una plataforma. Un ejemplo es el motor de búsqueda en donde el aumento del número de usuarios genera un beneficio para los anunciantes porque tendrá mayor audiencia (Lysnky, 2019).

- *Multi-homing*: es cuando los usuarios consumen diversos productos o se conectan a múltiples redes que cumplen todos los mismos o similares propósitos.

  Banda (2017) señala que el hecho de que los consumidores puedan utilizar varios motores de búsqueda o redes sociales al mismo tiempo y, por lo tanto, el riesgo de que estos queden encerrados en un solo servicio se reduciría, es un argumento falaz. Esta proposición fue argumentada en la decisión de Facebook/WhatsApp por la Comisión de la Unión Europea, al aducir que los usuarios instalaron y utilizaron en un mismo teléfono varios aplicativos para el mismo servicio de mensajería o chat[115]. No obstante, Banda (2017) considera que el hecho de que los usuarios tengan la posibilidad de descargar más aplicaciones no significa que todos sus amigos y familiares necesariamente los seguirán a esas aplicaciones. Por ello, argumenta que el *multi-homing*, quizá, reduzca los costos de cambio, pero aún los efectos de la red siguen siendo fuertes motivos cuando los usuarios prefieren una determinada empresa en lugar del resto.

---

[114] Esto está asociado a las plataformas consideradas como *two-sided* [de dos lados] o con *two- sidedness* [bilateralidad]. Esta dualidad de lados o tipos de actores es un elemento definitorio en lasplataformas, aunque muchas plataformas en la práctica tienen más de dos lados y, más bien, deberíanllamarse correctamente de múltiples lados (Crémer, de Montjoye, & Schweitzer, 2019).

[115] Esto alude al hecho de que, en 2014, la red social Facebook adquirió la plataforma de mensajería instantánea WhatsApp. Esta fue una decisión permitida por la Comisión de la Unión Europea porque Facebook aseguró que no sería capaz de vincular los datos de los usuarios en ambas plataformas, algo que terminó haciendo. Para más información ver: https://www.theguardian.com/business/2017/may/18/facebook-fined-eu-whatsapp-european-commission

Con todo, el *multi-homing* es importante al evaluar la competitividad de un mercado digital, pues, si bien está presente en mercados tradicionales, es, en su mayoría común en los mercados digitales. Por ejemplo, en Perú, las plataformas digitales para el servicio de *delivery* de comida, como Rappi, PedidosYa, UberEats, entre otras, ofrecen la misma funcionalidad (o casi la misma). No hay ningún costo por su uso (salvo los de envío o si se contratan membrecías *prime*), pero el beneficio de tener a más de una radica en el mayor acceso a más productos y/o restaurantes de comida ofertados.

- Presencia de grandes economías de escala[116]: según Crémer, de Montjoye, y Schweitzer (2019), está vinculado o explica la masiva existencia de servicios digitales gratuitos. Así, los tres autores indican que los consumidores suelen sentirse atraídos por un precio cero o gratuito; por ello, las empresas eligen no cobrar por su servicio a los consumidores y buscan obtener sus ingresos de la publicidad que les dirigen a los mismos. Así, los autores concluyen que gracias a la posibilidad de obtener grandes retornos a escala en las plataformas y a la atracción de los consumidores por lo gratuito, los proveedores deciden ofrecer sus servicios a los usuarios consumidores de su plataforma a precio cero y buscar obtener ganancias con otros servicios brindados al resto de los usuarios, que generalmente no califican como consumidores.

[116] Una economía de escala está enfocada a reducir costes tras el aumento de producción. Los costes generales de una cadena de producción disminuirán conforme aumente el número de productos o artículos fabricados en cada ciclo: "Es decir, los costes se sitúan por debajo de la producción, lo cual supone un necesario aumento de los beneficios" (MasContainer.com, 2020). Por ejemplo, "al invertir en nueva maquinaria, los gastos que hemos hecho por este concepto se amortizarán más fácilmente si el número de artículos fabricados aumenta" (MasContainer.com, 2020). Esto implica que en el entorno digital haya rendimientos extremos a escala, pues el costo de producción de los servicios digitales es mucho menos que proporcional al número de clientes atendidos; si bien no es novedoso como tal pues las fábricas suelen ser más eficientes que los minoristas más pequeños, el mundo digital lo lleva al extremo y esto puede resultar en una ventaja competitiva significativa (Crémer, de Montjoye, & Schweitzer, 2019).

Todas estas características llevan a algunos autores, como Lynsky (2019), a determinar que algunas empresas digitales poseen una posición ventajosa, en tanto gozan de *data power* [poder de datos]. Ello implica que el control sobre losdatos es decisivo y desencadena en potenciales problemas regulatorios. Lo anterior en tanto que, si bien todas las plataformas digitales tienen la capacidad de controlar y recopilar datos, algunas empresas poseen una capacidad superior para hacerlo como resultado del volumen y la variedad de datos disponibles. Es decir, en la práctica algunas plataformas ostentan gran dominio del mercado gracias a su notoria superioridad para controlar y tratar datos; lo que consecuentemente traería problemas en la competencia del mercado digital,siendo labor de la regulación atender eventuales abusos de dominio u otras fallasde mercado, tal como sucede en otros sectores.

Ante dicho contexto, Banterle (2019) resalta que los datos se han convertido en un recurso esencial y materia prima de la nueva economía digital[117]. Por ello, Banda (2017) precisa que el valor de la data depende altamente de su vinculación a otros *data sets* [conjuntos de datos][118]. Esta vinculación se explica en el sentido de que la calidad de las predicciones, producto del análisis de datos en múltiples áreas, se correlaciona tanto con el volumen de los datos utilizados en el análisis, como con la diversidad de sus fuentes, su precisión y su novedad (Gal y Rubinfeld, 2019).

Prueba de ello es que el volumen de datos recopilados para el año 2020, en todo el mundo, se estimó en 43 mil millones de *exabytes*. El Banco Mundial (BM)

---

117 Así, los datos son sin duda vistos como un *commodity* similarmente al petróleo porque ambos son fuentes de poder. Otros autores, más acertadamente, sugieren otras fuentes de poder con cualidades o propiedades más afines para ser comparadas, como lo son las materias primas por su masiva accesibilidad/recopilación y el poder ser reusadas varias veces, entre otras consideraciones. Para mayor información ver: https://truthonthemarket.com/2019/10/08/why-data-is-not-the-new-oil/#:~:text=2.,use%20by%20non-authorized%20parties.&text=This%20contrasts%20with%20oil%2C%20where%20complete%20excludability%20is%20the%20norm).

118 "Su traducción a nuestra lengua sería conjunto de datos y es una colección de datos habitualmente tabulada" (Balagueró, 2018).

señaló que dicha cifra se comparó con una pila de informes que van desde la Tierra hasta más allá de Plutón. También, se predijo que, en dicho año, treinta mil millones (30 000 000 000) de dispositivos de IoT, controlados por numerosos actores del mercado, estuvieron conectados a Internet, recopilando y utilizando datos (como se cita en Gal y Rubinfeld, 2019).

Sin embargo, la nueva economía de datos plantea nuevos desafíos y problemas sin resolver, sobre todo, en torno al acceso a conjuntos de datos grandes y diversos, así como al control que se les ejerce. Por ello, el factor clave e inicial es el acceso a los mismos, puesto que sirve para desarrollar una economía en torno al *Big Data*, el IoT y otras tecnologías inteligentes, donde una multitud de actores interactúan a diferentes niveles, durante la creación y generación de datos, ya sea para usar, compilar, crear, seleccionar, estructurar, enriquecer, analizar y agregarles valor (Banterle, 2019).

Este fenómeno, en el mercado de datos, es lo que la OCDE (2013) y otros académicos han compilado como cadenas de valor de datos. Su trascendencia radica en cómo los datos (personales y no personales) permiten la innovación de productos y servicios, la eficiencia de los procesos, nuevas formas de análisis y la creación de valor (de productores y usuarios en varios sectores de la economía). La aplicación de los marcos legales de protección de datos personales que les sean aplicables en cada país y sector específico afectarán directamente a la economía de las mismas.

Gal y Rubinfeld (2019) indican que la cadena de valor de datos[119] (personales y no personales) consta de los siguientes cinco (5) pasos de refinamiento:

- Recolección: los datos brutos personales y no personales se recopilan directamente o se compran en un mercado secundario de datos.

[119] Se sugiere tener en cuenta lo comentado en la primera sección del capítulo inicial, sobre la pirámide del conocimiento.

- Organización: donde los datos se deben estructurar en bases de datos y se convierten en información[120].

- Análisis: los datos estructurados se integran y procesan mediante algoritmos y, así, la información se convierte en conocimiento, como predicciones.

- Conservación: que incluye el archivo en formas recuperables.

- Uso: poner en práctica el conocimiento obtenido para la toma de decisiones en los mercados relevantes, es decir, el análisis obtenido de los datos estructurados conduce a una acción como la mejora de productos o servicios.

CERRE (2020) señala que, al continuar en la cadena de valor, los esfuerzos y las inversiones del propietario de los datos aumentarán y pueden estar protegidos por distintos derechos de propiedad intelectual. Como mencionan Banterle (2019) y la OCDE (2013), una amplia gama de partes interesadas está involucrada a lo largo de la cadena de valor, incluidos individuos, empresas, instituciones públicas, organizaciones sin fines de lucro, etc. Por su lado, algunos actores solo participan en partes seleccionadas de la cadena de valor. De ahí, nace el aumento del interés por proteger a la propiedad y los incentivos a invertir, que es parte del equilibrio a la hora de decidir imponer el acceso.

OCDE (2013) indica, como ejemplos de la participación en distintas partes de la cadena de valor a los corredores de datos, pues estos no suelen utilizar los datos personales, sino que los procesan y venden. Por el contrario, un ejemplo a las partes interesadas que participan en todos los pasos de la cadena de valor sería una aerolínea o minorista recopilando datos personales a través de un esquema de lealtad del cliente; luego, almacenarlos y agregarlos; y, finalmente, procesarlos y usarlos en su propio modelo comercial. (p. 11).

[120] Para CERRE (2020), los datos son la representación (digital) de señales que han sido recibidas o percibidas usando alguna sintaxis, tales datos se transforman en información solo si se combinan con semántica.

Por ello, los cinco (5) eslabones presentan barreras de entrada legales, tecnológicas o económicas (Gal y Rubinfeld, 2019). Las legales son, por ejemplo, las leyes de protección de datos personales que regulan su recopilación y tratamiento, los contratos que pueden contener cláusulas de exclusividad que prohíben la transferencia de datos, los derechos de propiedad intelectual, otros derechos de exclusividad[121] y los secretos comerciales. Así, específicamente, ante la legislación europea y a diferencia de otras legislaciones como la peruana, existe la figura del *sui generis data base right* para proteger el contenido de las compilaciones de bases de datos por quince (15) años, cubriendo incluso si estos han sido compilados de forma mecánica, en tanto haya habido una inversión sustancial en ello (siendo que el criterio de "inversión sustancial" se entiende de forma amplia). Esto es interesante, pues, si bien ante la legislación peruana la compilación de un banco de datos (estructura, pero no el contenido) podría ser protegida mediante derechos de autor, si dicha compilación es realizada de forma mecánica, ya no calificaría dentro del criterio de "originalidad", por lo que ya no sería aplicable esta protección de derechos de autor.

Las tecnológicas podrían ser cuando los datos están encriptados o si la data estructurada no es interoperable. Por último, las económicas implican que en la recopilación de datos se generen economías de escala y alcance[122] o efectos de red. Esto ocurre porque se recopilan masivamente datos en entornos de mercado multifacéticos contra servicios ofrecidos de forma gratuita con grandes efectos de red. El caso más claro son las redes sociales que recopilan los datos de los usuarios y los atraen fácilmente, dados los efectos directos de la red.

[121] Para mayor información ver: https://europa.eu/youreurope/business/running-business/intellectual-property/database-protection/index_en.htm

[122] La economía de alcance se avoca a las líneas de producción de un negocio y cómo se pueden ayudarentre ellas para garantizar la continuidad, la productividad y la financiación de un negocio. Por ejemplo, se puede pensar en una empresa dedicada a la venta de legumbres, frutas y al menaje de utensilios para el hogar. En caso de que alguna de las líneas de producción no diera los beneficios esperados, la otra podría suplir las deficiencias para evitar que deje de existir (MasContainer.com, 2020).

Asimismo, en el caso de efectos indirectos de red, un motor de búsqueda grande, como Google, atraerá más consultas porque pueden captar usuarios más fácilmente (Graef, Tombal y de Streel, 2019). Ambos casos, la red social y el motor de búsqueda, son perfectos para la presencia de economías de escala y alcance. Esto se da por la diversidad y cantidad de los datos recopilados, las cuales sirven para realizar un servicio óptimo y personalizado de publicidad dirigida *y micro-targeting*[123].

Un ejemplo de ello y de los actores e intereses involucrados en distintos niveles de la cadena de valor, es la disputa surgida entre los medios de comunicación del continente americano frente a las plataformas digitales. Los primeros sostienen que "los ingresos que financiaban el periodismo profesional son absorbidos por intermediarios que concentran más del 80% de la publicidad digital mundial (…) el sostenimiento del periodismo está en riesgo" (El Pais, 2021). Por ello, de acuerdo a El País (2021) piden que se "eviten prácticas abusivas en el mercado de la publicidad digital**"** y sean "investigadas y sancionadas para evitar una mayor concentración en los ingresos y en el uso de los datos personales", también a "los algoritmos, que condicionan la distribución de los contenidos y su llegada a la sociedad".

2.3.3 El mercado de datos (digital)

Como CERRE (2020) señala, comprender las implicancias económicas de la portabilidad de datos en el sector digital requerirá de un recuento de ciertas particularidades específicas de la economía global de los datos. Primero, esta última implica una economía de escala (asociada a la cantidad de los datos) y alcance (asociada a la variedad de los datos). Segundo, toda alusión en adelante a datos, se refiere a los datos digitales, definidos como información codificada y de lectura mecánica (Zech, 2016) y activo esencial en el *big data* o infraestructura de la economía digital (Ciuriak, 2018):

[123] Para mayor información ver: https://ami.org.co/medios-de-toda-america-llamamos-a-defender-el-valor-del-periodismo-profesional-en-el-ecosistema-digital/

- Una diferenciación trascendental gira en torno a cómo se adquieren los datos personales (CERRE, 2020):
    1. Proporcionados voluntariamente: son revelados explícita e intencionalmente, como el registrarse o publicar en redes sociales.
    2. Observados: son obtenidos del uso de un dispositivo, sitio web oservicio y el usuario puede no ser consciente de su recopilación, como las preferencias de navegación, o datos de ubicación móviles.
    3. Inferidos: producto del refinamiento y la recombinación de los dos (2) anteriores, como las puntuaciones de crédito según el historial financiero de una persona. Los datos inferidos es considerado conocimiento que proporciona información procesable.

  Por tanto, los datos inferidos son la base de la competencia entre empresas en el mercado de datos, mientras que los voluntarios y observados son sus insumos (*raw data* o datos brutos)[124]. Esto impacta en el contexto de la portabilidad, pues, por ejemplo, varias legislaciones, como el artículo 20° del RGPDP (2016), incluyen los datos proporcionados voluntariamente, pero no hay consenso sobre los datos observados; por su parte, el Grupo de Trabajo del Artículo 29 (2017) ha sugerido que los datos observados sean portables y se reafirme que los inferidos no estén comprendidos.

- Datos como bienes intangibles y no rivales vs. la rivalidad y exclusión en su recopilación: según, CERRE (2020), la no rivalidad y la exclusión son conceptos distintos que impactan en los beneficios y riesgos para el intercambio de datos y su portabilidad. En principio, los datos son intangibles y no rivales porque podrían ser recopilados, transferidos, divididos y utilizados por diferentes entidades al mismo tiempo a un costo marginal (Gal y Rubinfeld, 2019); sin embargo, son excluibles porque el responsable del tratamiento de datos puede imponer restricciones económicas, técnicas o legales para evitar su intercambio. Por ello, los datos específicos de cierto servicio o actividad en la práctica no pueden ser

[124] La diferencia entre datos, información y conocimiento implica, como CERRE (2020) señala, solo este último genera un "valor" agregado. (p. 51).

recopilados libremente por cualquier interesado, encontrándose concentrados en el mercado, mientras que, posteriormente, su consumo no resulta tan rival porque, en la práctica, suele ser objeto de transacciones económicas. Como consecuencia, existe concentración en pocos sitios web que son propiedad de una menor cantidad de empresas en la ubicación correcta para recopilar datos de los consumidores a gran escala con la capacidad de excluir al resto de agentes en el entorno digital[125]. Por ejemplo, con respecto al uso de rastreadores web o cookies, Englehardt y Narayanan (2016) determinaron que el primer millón de sitios web más empleados cuentan con *cookies* de terceros. El 70% de estos son de dominio de Alphabet/ Google y el 30% de Facebook. Así, estas dos *Big Techs* tienen una posición única para rastrear la actividad de los usuarios en varios sitios web de terceros. Todo parece indicar que esta situación se ha pronunciado aún más con el tiempo, ya que Google no permite más las *cookies* de terceros en su navegador Chrome. Algunos consideran que más allá de ser una medida para resguardar la seguridad y privacidad frente a la vigilancia en el entorno digital, la razón detrás sería reforzar su posición de dominio en el seguimiento web porque estas empresas cuentan con sus propios servicios para rastrear a los usuarios en la web, como *Google Analytics* (Barker, 2020).

Ello genera que la recopilación de datos observados, pero no los voluntarios, sea a menudo rival, porque para servicios clave (como motores de búsqueda o redes sociales), el mercado está altamente concentrado y solo pocas empresas pueden rastrear la actividad de los usuarios en la web. Por ende, los datos observados no están disponibles de forma ubicua, lo que genera la necesidad de compartir datos en el entorno digital. Esto se vincula con la

[125] Para mayor información ver:

- https://www.ft.com/content/169079b2-3ba1-11ea-b84f-a62c46f39bc2.
- https://www.grupoendor.com/google-cookies-de-terceros/

idea de la cadena de valor y la participación de múltiples actores en distintas etapas como parte del negocio en conseguir su acceso[126].

- Rivalidad en el valor derivado de la data: según CERRE (2020), el valor económico de los datos dependerá de cuántos sujetos tengan acceso a los datos o puedan obtener los mismos conocimientos a partir de dichos datos[127]. Si el intercambio de datos tuviera costos de transacción cero para los consumidores, generaría que empresas, eventualmente, posean conjuntos de datos idénticos y que solo un comprador de datos esté potencialmente interesado en adquirirlos por única vez, pues cada conjunto de datos actuaría como sustituto perfecto del otro en el mercado. Aunque el consumo de datos no es rival, su valor económico derivado sí lo es. Se dice que esto es un motivo para no permitir a los titulares de los datos personales portar sus datos, ya que destruiría los incentivos para recopilarlos al inicio y haría más deseable esperar a que sean transferidos por otros.

  No obstante, CERRE (2020) aclara que tal postulado no distingue entre datos y el conocimiento generado, porque se está enfocando en los intermediarios de datos dedicados a recopilar y vender aquellos que sean brutos. A pesar de que dos empresas pueden tener acceso al mismo conjunto de datos brutos (es decir, datos voluntarios y observados), podrían generarse conocimientos distintos (es decir, datos inferidos), los cuales son la base para competencia. Estos podrían ser vendidos a terceros en el mercado de datos o combinados con otros datos disponibles por la misma empresa. De esta manera, se generarían *data sets* enriquecidos que podrían venderse como *data sets* únicos, superando a la competencia dentro el mercado de datos. Segundo, no se han considerado los costos intrínsecos de transacción

[126] Al respecto, el acceso a datos puede tener lugar en diferentes niveles de la cadena de valor, es decir,a datos sin procesar. Después, puede llevar a cabo otras operaciones posteriores, es decir, estructurar, analizar y utilizar los datos; puede solicitarse acceso a la estructura y, luego, posiblemente, recopilar y analizar los datos, o a la *suite* completa, es decir, los datos recopilados, estructurados y analizados para tomar su propio curso de acción (Graef, Thombal & de Streel, 2019).

[127] Por ejemplo, CERRE (2020) indica que, tanto Ishihashi (2019) como Gu (2018), mostraron, mediante un modelo de teoría de juegos, que el valor de los datos recolectados de los consumidorespuede caer significativamente (en sus modelos teóricos hasta a cero) si más de una empresa lo posee.

de vender datos personales en el mercado, como el cada vez más engorroso cumplimiento a normativas de datos personales aplicables al compartir *data sets* con otra empresa, entre otros.

Finalmente, un intercambio más frecuente de datos brutos probablemente hará que el mercado de intermediarios de datos se vuelva más competitivo y menos lucrativo, pero esto no destruiría los incentivos para competir sobre la base de conocimientos derivados de los datos. Más bien, a medida que los datos brutos se vuelvan más frecuentes, es probable que el foco de la competencia pase de la recopilación a la analítica, estimulando la innovación de análisis de datos basada en conocimiento. Esto es más deseable que la competencia a nivel más básica de recopilación de datos, actualmente concentrada y con fuertes efectos de red.

- Tener acceso a más datos voluntarios[128] y observados[129] producirá una mejor calidad de aquellos inferidos con mayores oportunidades de ganancias, por lo que el ámbito de aplicación de su portabilidad respecto de qué datos personales comprenderá será crucial desde la perspectiva económica (CERRE, 2020).

[128] Derivan de la participación humana directa por lo que pueden ser inexactos, estar incompletos y quedar obsoletos, por ejemplo, al enviar información incorrecta intencional o involuntariamente. Su precisión es esencial para la calidad del servicio. Por ello esto resulta ser un incentivo en la industria para que los consumidores brinden datos lo más precisos posibles, con el objetivo de obtener mejores -y más precisos- servicios, por ejemplo, de recomendación o sugerencias. Sin embargo, sí suelen estar estructurados porque se recopilan, generalmente, de forma estructurada, como en formularios o botones de "me gusta", siendo una entrada directa para generar datos inferidos.

[129] Son menos propensos a la manipulación deliberada porque se derivan del comportamiento y sensores reales. Por ello, tienden a ser más completos y oportunos al registrarse automáticamente. No obstante, su precisión e integridad depende del contexto, por ejemplo, clics deliberados en un sitio web que generen cookies analíticas o, el caso de sensores de GPS en condiciones geográficas y climáticas adversa pueden producir ciertos errores. Además, suelen estar menos estructurados y deben "limpiarse" para derivar en conocimientos procesables.

La calidad de los datos se puede medir por su aptitud para el uso (qué tan adecuados son para obtener los conocimientos deseados), su precisión (para representar los hechos), su integridad, su rapidez en obtención y su desactualización. Por su parte, Gal y Rubinfeld (2019) afirman que la calidad de las predicciones en aplicaciones se correlaciona con el volumen de los datos utilizados en el análisis, la diversidad de sus fuentes, su precisión y actualidad. Para los autores, la calidad del conocimiento minado de la data está afectada por las cuatro principales características de la data: volumen (cantidad de datos en un *dataset*), velocidad (actualidad de la data), variedad (en base a la cantidad de diferentes fuentes de las que se obtienen), veracidad (precisión).

Con respecto al análisis masivo de datos, estudios sugieren que hay una escala mínima requerida, mientras más grandes son los *data sets*, más beneficios proporcionan[130], pero esos beneficios también disminuirían marginalmente a medida que se alcanza o supera cierto umbral de tamaño. Por ejemplo, en la publicidad en línea, Lewis y Rao (2015) encuentran que solo grandes cantidades de datos permiten a las empresas medir si las campañas publicitarias son realmente exitosas. Así, CERRE (2020) considera que la presencia de economías de escala nace de la recolección y análisis de datos en los que se necesita una suerte de umbral mínimo (masivo), en cuanto a cantidad y calidad, para obtener adecuados beneficios en el análisis de datos.

Se trae a colación que las economías de datos funcionan como economías de escala y alcance, por lo que mientras más cantidad y variada sea la data, el conocimiento que será extraído será mejor, más preciso y valioso. Así, Mayer-Schönberger y Padova (2016) afirman que el valor de los datos puede mejorarse en gran medida si se tienen y analizan más, y si se combinan con otras fuentes de datos. Por ende, se pueden crear externalidades positivas con respecto a otros *data sets*, ya que un algoritmo puede aprender de un *data set* con alto valor para realizar

130 Cuando distintos atores hacen referencia a grandes o largos *data sets* y/o la capacidad de juntarlos, están aludiendo al fenómeno del Big Data.

tareas que, luego, replicará en otros similares, generando una transferencia de aprendizaje (Gal y Rubinfeld, 2019)[131].

Finalmente, Gal y Rubinfeld (2019) afirman que sucede un bucle o ciclo de retroalimentación en términos de escala y alcance, pues tener mejores y más datos genera mejores predicciones, que se traducen en mejores productos; y, mejores algoritmos que también producen mejores productos en términos del *data set* original y del aprendizaje que se transfiere.

2.3.4 Derecho a la libre competencia en el mercado digital

Ante lo expuesto, resulta relevante mencionar la función del derecho a la competencia, encargado de proteger el bienestar del consumidor contra el comportamiento anticompetitivo en el mercado. En el caso peruano, el artículo 1° del Decreto Supremo Nº 030-2019-PCM, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley de Represión de Conductas Anticompetitivas [T.U.O. de la LRCA], indica que su finalidad es prohibir y sancionar "las conductas anticompetitivas con la finalidad de promover la eficiencia económica en los mercados para el bienestar de los consumidores".

Si bien los mercados tradicionales tampoco funcionan en competencia perfecta[132], incluso, a veces, las empresas cuentan con un importante poder de mercado[133] que les permite neutralizar o superar la posibilidad de competencia,

[131] Como ejemplo, los autores señalan que Facebook pudo crear un mejor algoritmo de reconocimiento facial porque su algoritmo podía aprender de un vasto conjunto de datos que tenía un alto nivel de veracidad, es decir, las abundantes fotos subidas a su red social por parte de todos los millones de usuarios en el mundo. Para mayor información ver: https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/

[132] En Perú, el INDECOPI (2013) "señala que la competencia perfecta implica presencia de productos homogéneos, gran número de vendedores y compradores, información perfecta (completa, simétrica, oportuna y suficiente para tomar decisiones adecuadas), ausencia de barreras importantes de acceso al mercado" (p. 15).

[133] Según Bishop y Walker, es la capacidad de una empresa para fijar precios por encima de los costos marginales que serían el resultado de competencia perfecta (como se cita en INDECOPI, 2013). Si

en el sector digital, se evidencian marcadas tendencias asimétricas a favor de ciertas empresas frente a sus competidores (si los hay) y sus consumidores bajo particularidades que, como se verá, difieren de los mercados tradicionales. Ante ello, la OCDE (2019b) ha recomendado que, para fomentar la confianza informada en dichos mercados, es importante que existan y se apliquen adecuadamente las leyes de competencia efectiva, protección del consumidor y de protección de datos.

Sin embargo, también se requiere de cooperación entre tales autoridades de competencia, datos y protección del consumidor, así como de reformas regulatorias favorables a la competencia y a iniciativas privadas para un trato integralmente justo a los consumidores en línea.

Como antesala, a nivel mundial, hay un puñado de empresas multinacionales digitales que son dominantes: Google, Facebook, Microsoft, Amazon y Apple, sin perjuicio de otras. Por tanto, los mismos riesgos asociados con un monopolio tradicional que explota su posición de dominio pueden surgir en el mercado digital, solo que con alcance mundial. Además, las plataformas suelen ser diversas e integradas en ecosistemas. Por ello, determinar la forma en que compiten requerirá de un análisis particular en cada caso (Crémer, de Montjoye & Schweitzer, 2019). Esto, de entrada, colisiona con la idea de economía (social) de mercado amparada en la CPC y la aspiración al modelo de competencia perfecta, con infinitos compradores, vendedores y los beneficios que trae como precios más bajos, mejores productos, más opciones y eficiencia (Whish & Bailey, 2018). De esta manera, el bienestar del consumidor digital podría estar en riesgo.

bien toda empresa tiene cierto grado de poder de mercado, pues no existe la competencia perfecta, lo importante es identificar cuánto poder de mercado se tiene para evaluar si podría generar una afectación negativa.

El primer paso para que la Comisión de Defensa de la Libre Competencia (CDLC)[134] pueda determinar la existencia de una infracción legal, es definir el mercado relevante, que es "evaluar si existen o no alternativas para el cliente o consumidor o, en otras palabras, si este se encuentra 'cautivo' de su proveedor habitual" (INDECOPI, 2013, p. 19); si la respuesta es afirmativa, entonces, el proveedor tiene posición de dominio. Esto comprende, según el artículo 6° del T.U.O. de la LRCA (2019), al mercado de producto relevante, que es el bien o servicio materia de la conducta investigada y sus sustitutos, se requiere de un análisis de sustitución por parte de la autoridad de competencia en la que se evalúan preferencias de clientes/consumidores, características, usos y precios de posibles sustitutos, las posibilidades tecnológicas y el tiempo requerido para la sustitución de los productos o servicios en cuestión; y, al mercado geográfico relevante, que implica hallar el conjunto de zonas geográficas donde están ubicadas las fuentes alternativas de aprovisionamiento del producto relevante, considerando costos de transporte y barreras al comercio existentes, etc.

No obstante, en negocios como redes sociales, *market places* y motores de búsqueda u otros, definir el mercado relevante bajo tales criterios resulta complejo y limitado. Estos negocios son ubicuos y no cuentan con presencia física para la mayoría de sus operaciones, por lo que el criterio de mercado geográfico es desfazado. Además, muchas veces, los servicios brindados por plataformas digitales no se reconocen a sí mismos como servicios existentes en mercados tradicionales, sino como otros *sui generis* o distintos; las redes sociales no serían medios de comunicación, los aplicativos para servicio de taxi no serían servicios de transporte sino intermediadores digitales de servicios de transporte; y, las *fintech* serían servicios intermediadores de servicios financieros, pero no financieros.

[134] La CDLC del INDECOPI es el órgano con autonomía técnica y funcional encargado del cumplimiento del T.U.O de la LRCA (2019) en todos los mercados, con excepción del mercado de servicios públicos de telecomunicaciones, a cargo del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL). En ejercicio de sus atribuciones, puede determinar la responsabilidad de las empresas y sus ejecutivos por las infracciones a la Ley, imponer multas y dictar medidas correctivas (INDECOPI, 2020).

Además, la constante aparición de nuevos modelos comerciales o actualizaciones de los ya existentes, de manera casi inmediata, dificulta determinar cuáles son las "posibilidades tecnológicas y el tiempo requerido para la sustitución" (artículo 6°, T.U.O. de la LRCA, 2019), en plataformas digitales y, mientras más grandes sean estas últimas, el sesgo y la complejidad de hacerlo será aún mayor: los mismos datos (o al combinarse con otros *data sets*) juegan un rol decisivo, pues son materia prima que puede ser usada en múltiples mercados infinitamente directa e indirectamente en casi todos los mercados digitales. Solo basta hallar puntos de encuentro o a qué otros *data sets* y algoritmos podrían serles útiles.

También, la mayoría de productos y servicios son ofrecidos a los consumidores gratuitamente o en modalidades[135] que no necesariamente buscan un pago económico al corto plazo. Estos pueden tener otros fines como el aumentar su presencia en mercados conexos[136], pudiendo soportar grandes pérdidas para acceder a datos personales de los usuarios[137] y brindar otros servicios a clientes a los que les trasladarán los costos, como las redes sociales gratuitas o subsidiadas a los usuarios, pero con espacios publicitarios para empresas o aplicativos de taxi que cobran una tarifa únicamente al conductor por cada viaje. Así, en noviembre de 2019, el motor de búsqueda Google anunció su adquisición sobre la marca Fitbit orientada a la salud que produce dispositivos/relojes de seguimiento del estado físico, lo que le permitiría acceder a una nueva área del

135 Incluso, se afirma que el modelo de negocio más usado en el entorno digital es el *data as payment* o pago con tus datos personales, pues el verdadero activo para las empresas tecnológicas es contar con mayor cantidad de datos y, así, enriquecer sus algoritmos, conocimiento y mejorar la toma de decisiones respecto a otras actividades de negocios asociadas en las que transan.

136 Para mayor información ver: https://telecoms.com/504015/why-is-google-so-interested-in-fitbit/

137 CERRE (2020) indica que existe una creciente evidencia empírica del establecimiento de *kill zones* [zonas de muerte] (p.62), en torno al modelo de negocio central de empresas digitales dominantes. Esto significa que las empresas innovadoras y nuevas, que podrían convertirse en competidores de una gran empresa de tecnología en particular, pueden terminar compradas por ella o esta última rápidamente podrá incorporarla en su propio servicio dado que el operador establecido tiene una ventaja comparativa de facto en relación con las nuevas empresas o las empresas más pequeñas debido a sus recursos financieros mayores, sus economías de escala y los efectos de red (CERRE, 2020). Esto tiene relación con el ejemplo señalado sobre las tensiones entre Snapchat e Instagram.

mercado y realizar nuevas inversiones como cuidado de la salud e incluso ciudades inteligentes (Davies, 2020).

De esta manera, definir los bienes o servicios sustitutos puede ser arriesgado. Por ejemplo, en 2013, Facebook intentó, sin éxito, comprar la aplicación Snapchat; no obstante, ya había adquirido Instagram, en 2012. La función inicial de Snapchat, por la cual se hizo popular, era compartir historias (*stories*), a través de *My Story*, en 2013, y, luego, por sus filtros y funcionalidades innovadoras en sus historias[138]. Hasta ese momento, Instagram, si bien competía con la mensajería instantánea, no podía respecto a *My Story* y sus filtros. Sin embargo, en 2016, tras copiar otras funcionalidades de Snapchat, como mensajes de texto o videos cortos que se eliminan después de vistos por el remisor, lanzó *Instagram Stories* con las funcionalidades y filtros muy similares a Snapchat[139]. Hoy, la presencia de Instagram es abrumadora y muestra como no podía ser competidora directa sobre funcionalidades específicas de Snapchat, pero gracias a las facilidades tecnológicas, recursos económicos masivos y superiores y su gran presencia preexiste en redes sociales, pudo adicionar las mencionadas funcionalidades (casi idénticas) para tomar presencia en un servicio conexo y relegar a su competidora.

Definir el bien o servicio materia de análisis también es complejo. Generalmente, las plataformas son *two-sided* o *multi-sided*, como se dijo, tienen usuarios de distintas categorías, como proveedores y consumidores y el más valioso es subsidiado y el otro paga por ello. Asimismo, existen los citados prosumidores, consumidores y proveedores del contenido propio que generan en la plataforma digital y parte de la cadena de negocio. A veces, la plataforma resulta siendo un férreo competidor directo de sus usuarios en otro servicio. La plataforma de venta de productos *Amazon*, gratis a consumidores (salvo *Amazon Prime*), cobra a proveedores, pero resulta ser un competidor potencial, pues

138 Para mayor información ver: https://www.ionos.es/digitalguide/online-marketing/redes-sociales/instagram-stories-vs-snapchat-stories-una-comparativa/

139 Para mayor información ver: https://www.elespanol.com/omicrono/software/20170516/llegan-filtros-instagram-copia-descarada-snapchat/216479154_0.html

emplearía (sin consentimiento de empresas clientes), su data para copiar productos *best sellers* y patrones de éxito para entrar como proveedor en su plataforma. Controversialmente, su director ejecutivo, Jeff Bezos, ante el Subcomité de Defensa de la Competencia del Poder Judicial de la Cámara de Representantes en Estados Unidos de América, declaró que no pueden garantizar que su política contra uso de datos del vendedor no haya sido violada[140].

Los autores como Crémer, de Montjoye y Schweitzer (2019) afirman que los límites del mercado pueden no ser tan claros como en la vieja economía, en tanto, que la interdependencia de los mercados digitales se convierte en una parte crucial del análisis, *contrario sensu* al papel tradicional de la definición del mercado abocada a aislar los problemas o mercados. Por ende, debe enfatizarse menos la definición del mercado a favor de teorías del daño y la identificación de estrategias anticompetitivas interdisciplinarias.

El segundo paso es determinar el dominio en el mercado que, según el artículo 7.1º del T.U.O de la LRCA. (2019), implica lo siguiente:

> [U]n agente económico (…) en un mercado relevante (…) tiene la posibilidad de restringir, afectar o distorsionar en forma sustancial las condiciones de la oferta o demanda en dicho mercado, sin que sus competidores, proveedores o clientes puedan, en ese momento o en un futuro inmediato, contrarrestar dicha posibilidad, debido a factores tales como: a) una participación significativa en el mercado relevante, b) las características de la oferta y la demanda de los bienes o servicios, c) el desarrollo tecnológico o servicios involucrados, d) el acceso de competidores a fuentes de financiamiento y suministro así como a redes de distribución, e) la existencia de barreras a la entrada de tipo legal, económica o estratégica, f) la existencia de proveedores, clientes o competidores y el poder de negociación de estos.

[140] Para mayor información ver: https://www.brookings.edu/blog/techtank/2020/08/11/the-tech-antitrust-hearings-are-over-whats-next-for-enforcement/

Adicionalmente, el INDECOPI (2013) indicó que dicho poder de mercado puede obtenerse por fuentes lícitas o ilícitas, como la eficiencia económica, que impulsa a las empresas a lograr ganar la preferencia de los clientes para ser más reconocida o incluso la única que quede en el mercado; concentración de empresas; ventajas creadas por ley, en tanto las normas legales o las decisiones de las autoridades pueden reducir la posibilidad de ingreso de nuevas empresas al mercado, haciendo más costosa su entrada o impidiéndola de modo absoluto a través del otorgamiento de derechos exclusivos de operación (un ejemplo es el sector de telecomunicaciones o minería); y, la conducta de agentes, impidiendo inválidamente que rivales compitan, forzándolo a competir en condiciones desiguales, o coordinando con competidores el comportamiento para lograr un poder de mercado artificial.

Sin embargo, la sola tenencia de una posición de dominio no es una conducta ilícita. Ello solo sucederá si la autoridad determina alguna de las infracciones tipificadas en el T.U.O. de la LRCA (2019), como abuso de posición de dominio, y prácticas colusorias horizontales y verticales. Por ser de mayor interés a esta investigación, únicamente, se abordará el primer supuesto.

Para el abuso de dominio[141], debe probarse que el agente económico con posición dominante en el mercado relevante "utiliza esta posición para restringir de manera indebida la competencia, obteniendo beneficios y perjudicando a competidores reales o potenciales, directos o indirectos, que no hubiera sido posible de no ostentar dicha posición" (artículo 10.1º, T.U.O. de la LRCA, 2019).

Los artículos 10.2º y 10.3º del T.U.O. de la LRCA (2019) indican que se materializa en conductas exclusorias que afectan a competidores reales o potenciales al negarse injustificadamente a satisfacer demandas de compra o venta; aplicar condiciones desiguales para prestaciones equivalentes que injustificadamente desfavorezcan a unos competidores frente a otros; subordinar

[141] Nótese que las conductas de abuso de posición de dominio son prohibiciones relativas. Para verificarsu existencia como infracción, la CDLC deberá probar su existencia y además que tiene, o podría tener, efectos negativos para la competencia y el bienestar de los consumidores.

la celebración de contratos a la aceptación de prestaciones adicionales que no guarden relación con su objeto; obstaculizar injustificadamente la entrada o permanencia de un competidor en una asociación u organización de intermediación; establecer, imponer o sugerir contratos de distribución o venta exclusiva, cláusulas de no competencia o similares, injustificadamente; utilizar abusiva y reiteradamente acciones judiciales o administrativas para restringir la competencia; incitar a terceros a no proveer bienes o prestar servicios, o a no aceptarlos; y, otras que impidan o dificulten acceso o permanencia de competidores actuales o potenciales, ajenas a la eficiencia económica.

En base a todo lo expuesto, el determinar la existencia de posición de dominio y el subsecuente abuso en línea, también, puede ser complejo por el antecedente de las trabas para determinar el mercado relevante y por la dificultad para identificar adecamente la dinámica comercial entre todos los agentes del mercado (consumidores y proveedores).

Primero, si no hay cobro monetario a usuarios, pues se monetizan los servicios a través de un mercado publicitario paralelo, ¿cómo podría identificarse, por ejemplo, un abuso mediante aumentos significativos del precio? Así, Graef, Wahyuningtyas y Valcke (2015) afirman que la calidad de los servicios a los usuarios depende de la naturaleza y cantidad de los datos recopilados, es decir, de su base de usuarios. Por ello, los proveedores de plataformas no están dispuestos a dar acceso a la información recopilada de usuarios, como sucede en el caso de las redes sociales, donde los sitios webs de terceros, pese a contratar servicios como publicidad dirigida, anuncios y otras estadísticas de monitoreo y preferencias, no pueden adquirir directamente la información del usuario. Como muestra de ello, las vigentes Condiciones del servicio de Facebook (2020) indican lo siguiente:

> No cobramos por el uso que haces de Facebook ni de los otros productos y servicios que abarcan estas Condiciones. Por el contrario, los negocios y las organizaciones nos pagan para que te mostremos anuncios de sus productos y servicios. Al usar nuestros Productos, aceptas que podemos mostrarte anuncios que consideremos que te resultarán relevantes para ti y tus

> intereses. Usamos tus datos personales como ayuda para determinar qué anuncios mostrarte.
>
> No vendemos tus datos personales a los anunciantes ni compartimos información que te identifique directamente (como tu nombre, dirección de correo electrónico u otra información de contacto) con los anunciantes, a menos que nos des tu permiso expreso. Por el contrario, los anunciantes pueden proporcionarnos datos como el tipo de público que quieren que vea sus anuncios, y nosotros mostramos esos anuncios a las personas que pueden estar interesadas en ellos. Proporcionamos a los anunciantes informes sobre el rendimiento de sus anuncios para ayudarlos a entender cómo interactúan las personas con su contenido [subrayado añadido].

Así, la UNCTAD (2019) afirma que la aplicación del criterio del bienestar del consumidor en el comercio en línea es compleja. Ello, debido a rápidas fluctuaciones de precios y la posibilidad de los algoritmos de fijar precios personalizados, a veces, discriminatorios. Además, muchos de los servicios, aparentemente gratuitos, se pagan proporcionando datos personales. Por otro lado, UNCTAD (2019) menciona que la "fijación de precios predatorios, que es un elemento fundamental de la estrategia comercial que siguen las plataformas que dominan la venta en Internet para crecer y monopolizar el mercado" (p. 5). Al inicio, parece positivo pagar menos o no hacerlo. Si los competidores quedan excluidos podrán aumentar los precios discrecionalmente, disminuyéndose la oferta. Por ello, la UNCTAD (2019) concluye que el bienestar del consumidor debería entenderse ampliamente e incluir criterios como la privacidad y la posibilidad de elegir del consumidor, la protección de los datos personales, costos asociados al cambio y el efecto de captura por las plataformas dominantes.

Segundo, Banda (2017) señala que otro problema con las herramientas de competencia actuales es la determinación de la cuota de mercado. Esta es en principio un indicador tradicional del poder, pues las cuotas de mercado muy grandes proporcionarán evidencia de dominio, pero que, en entornos digitales ha demostrado ser insuficiente. Al respecto, autoridades como la Cuarta Sala del Tribunal General (2013), en la Sentencia en el asunto T-79/12, entre Cisco

Systems Inc. y Messagenet SpA, contra la Comisión Europea, apoyada por Microsoft Corp., lo advirtieron por los siguientes motivos:

> [e]l sector de las comunicaciones de particulares [en Internet] es un sector reciente en plena expansión que se caracteriza por ciclos de innovación cortos y en el que las cuotas de mercado altas pueden resultar efímeras. En ese contexto dinámico las cuotas de mercado elevadas no son necesariamente indicativas de un poder de mercado ni, por tanto, del perjuicio duradero para la competencia. (n. 69).

Por ello, como un indicador alternativo para los mercados de innovación, tanto para futuras fusiones de datos personales o casos de abuso de dominio relacionados con datos personales, Graef propone considerar la competencia en la innovación (como se cita en Banda, 2017). Ello implicaría que en los casos enque empresas digitales estén interesadas en adquirir empresas con grandes conjuntos de datos personales, deberán considerarse el potencial tanto para crearnuevos productos sobre estos, como para invertir en investigación.

Tercero, estos mercados tienen un perfil multifacético, con efectos de red directos e indirectos. Esto puede favorecer más la concentración del mercado y actuar como barreras de entrada frente a otras plataformas que brinden el mismo servicio si no cuentan con los mismos recursos para ser igualmente competitivos por no ofrecer el mismo nivel de calidad que los operadores tradicionales (Laserre y Mundt, 2017). Incluso si se pudiera migrar al competidor con costos de cambio bajos o nulos, lo que importará a los consumidores es el nivel real de fidelización y experiencia en la plataforma, generado gracias a herramientas de análisis de perfiles para determinar preferencias, segmentaciones y predicciones que generan servicios personalizados en base a la experiencia previa.

Ello explica la proliferación de ecosistemas que lo abarcan todo: una plataforma termina brindando múltiples servicios y compra nuevos participantes a medida que comienzan a prosperar (Laserre y Mundt, 2017). Si bien en principio puede ser competidora directa con otra plataforma respecto a una funcionalidad, el beneficio de acceder a una sola plataforma para tener acceso a múltiples

funcionalidades es algo que no debe dejarse de lado como un factor relevante. Por ejemplo, Google tiene una amplia gama de productos y servicios que van mucho más allá del original motor de búsqueda[142].

Como consecuencia de los tres (3) anteriores, algunos propugnan otros impactos negativos atípicos como violaciones de la privacidad o prácticas excesivas de procesamiento de datos que indiquen el abuso de dominio. Para ello, como se anticipó, el poder de mercado digital estaría demostrado en el poder de los datos. Para Lynskey (2019) implica utilizar el acceso a volúmenes y variedades importantes de datos personales para aumentar la elaboración de perfiles algorítmicos más reveladores que exacerban las asimetrías de poder entre individuos y entidades con poder de datos; influir, manipular o discriminar a las personas; e, incluso influir en la opinión pública determinando la información presentada a usuarios, lo que alberga cuestiones de interés público más amplias que solo la defensa de la competencia[143].

---

[142] Algunos de los productos y servicios de Google son Maps, Traductor, Chrome, Youtube, Youtube Music, Google TV, Chromecast, Pixel, Casa conectada, Pixel Slate, Google Wifi, Sistema operativo Android, Wear OS by Google, Android Auto, Chromebook, Gmail, Mensajes, Google Duo, Google Chat. Fotos, Contactos, Keep, Calendar, Documentos, Hojas de Cálculo, Presentaciones, Drive, Google Ads, Adsense, Google My Business, Analytics, Académico, Alertas de Google, Android, Android Auto, Android TV, Asistente de Google, Brocha Virtual, Cardboard, Chrome enterprise, Dibujos, Earth, Expediciones de Google, Finance, Formularios, Gboard, Google Arts & Culture, Google Cast, Google Classroom, Google Cloud Print, Google Express, Google Fi, Google Fit, Google Fonts, Google Meet, Google One, Google Play, Google Play Book, Waze, Haungouts, Travel, Play Protect, entre muchos otros. Para mayor información ver: https://about.google/intl/es/products/

[143] El caso emblemático es el mencionado anteriormente "Escándalo Cambridge Analytica". Sin embargo, existen muchísimos casos más; por ejemplo, el 2020 el Secretario General de la OEA, Luis Almagro, y el Vicepresidente de Asuntos Globales y Comunicaciones de Facebook, Nick Clegg, firmaron un acuerdo marco de cooperación para trabajar en iniciativas incluyendo la integridad electoral. Para mayor información ver: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-026/21
Así, en el curso de las Elecciones Generales 2021 en Perú, Facebook llevó a cabo una serie de acciones para aportar transparencia a la publicidad política y electora en sus distintas plataformas, incluyendo Instagram y WhatsApp. Para mayor información ver:

Cabe reflexionar que es de interés público cómo las redes sociales fomentan la polarización y que los algoritmos están diseñados no para mostrar primordialmente sucesos o contenido objetivo, sino para buscar el *engagement* con el usuario. Así, se identifican contenidos (académicos, políticos o que inspire emociones) para que los usuarios pasen el mayor tiempo posible en redes sociales y anunciarles mayor publicidad dirigida. Mcnamee (2019)[144] afirma que, si una persona considera que la tierra es plana, entonces los algoritmos buscarán mostrar contenidos que sean afines. Esto podría generar que el usuario refuerce creencias, afinidades, sensaciones o sentimientos independientemente de lo nocivas que sean para la sociedad. Ante ello, muchos analíticos han explicado que, en los últimos años, las redes sociales han contribuido mundialmente a generar polarización entre las sociedades y parcialización o limitación al dejar de informarte sobre posturas distintas y contrarias[145].

Un caso extremo es Birmania, donde Facebook fue clave para la limpieza étnica contra los *Rohingya*, vía divulgación del discurso islamófobo impartido por el clero budista y propaganda nociva por la dictadura militar. Hoy, han vuelto a caer en una dictadura militar y se reportan muchísimas muertes y violaciones a los derechos humanos de la población civil, atribuidas al gobierno golpista militar que no aceptó la derrota en las recientes elecciones. En ello, la Internet y redes sociales, como Facebook, sirven como canal de comunicación entre los ciudadanos y el mundo, pues ayuda a divulgarla grave situación. Aquí, se trata de

https://elperuano.pe/noticia/117541-elecciones-2021-facebook-facilita-la-participacion-y-fomenta-la-transparencia

144 Roger Mcnamee fue mentor temprano de Mark Zuckerberg, el creador de Facebook, y uno de los primeros inversionistas de dicha empresa. Mcnamee ha revelado que, en el pasado, incluso aconsejó a Zuckerberg no vender Facebook. Para mayor información ver: https://www.lavanguardia.com/tecnologia/20190220/46573030031/mcnamee-facebook-zuckerberg-red-social-inversor-criticas.html

145 Para mayor información ver: https://www.lavanguardia.com/tecnologia/20181107/452785416274/facebook-myanmar.html

cortar el contacto internacional y controlar los medios de comunicación y las redes sociales, identificando y sofocando detractores[146].

2.3.5 Libre competencia y acceso a datos

Continuando con el fenómeno del poder de los datos, en situaciones específicas, su acceso se ha considerado indispensable en atención a los intereses legítimos[147]. Esto sucede ante el desarrollo de mercados complementarios, secundarios o de posventa, debido a que se pretende proteger el ecosistema o cadena de valor. Un segundo caso es cuando las especificidades o granularidad de los datos necesarias para su utilidad por parte de otros responsables de tratamiento, está en juego; aunque este supuesto a menudo puede entenderse como comprendido en el anterior abocado a proteger la cadena de valor[148]. A raíz de ello, algunas autoridades han propuesto imponer obligaciones que garanticen el acceso a los datos e, incluso, su interoperabilidad (Krämer & Wolfahrt, 2017).

Dicha iniciativa tiene como antecedente legal e histórico que autoridades, como la Comisión Europea y la Corte Suprema en Estados Unidos de América, han decidido jurisprudencial y normativamente que ciertas empresas con poder de dominio deben estar sujetas a ciertos deberes inherentes a su posición en el mercado. Bajo tal lógica, en el sector digital tales deberes se verían traducidos en

---

[146] Para mayor información ver: https://www.elobservador.com.uy/nota/el-otro-frente-del-golpe-de-estado-en-birmania-internet-y-las-redes-sociales-2021217124551

[147] Krämer y Wolfahrt (2017) advierten que es necesario distinguir entre diferentes formas de datos, niveles de acceso a los datos y usos de los datos. Así, en varios entornos el acceso a los datos no será indispensable para competir. Por ello, las autoridades públicas deberían abstenerse de intervenir, siendo preferible soluciones basadas en el mercado (Krämer & Wolfahrt; 2017).

[148] Los datos granulares son datos que están en pedazos, los más pequeños posible para ser más definidos y detallados. Estos se pueden moldear de cualquier forma que requiera el científico de datos o el analista, agregarse, desglosarse, combinarse con fuentes externas y administralos,atendiendo las necesidades de diferentes situaciones. Si no están granulados, como un campo de nombre o dirección que se guarda como un todo, entonces será muy difícil extraerlos y analizarlos en grandes porciones. (Techopedia, s.f.). Para mayor información ver: https://www.techopedia.com/definition/31722/granular-data

que los agentes en el mercado garanticen el acceso e interoperabilidad[149] a sus datos y demás servicios en circunstancias en las que, de pretender negarse, consecuentemente se afectaría a la competencia en dicho mercado.

Por ello, se buscará abordar esta posibilidad a efectos de analizar en qué medida dicha figura legal incide en el mercado de datos digital y cómo debe garantizar el acceso a los mismos, incluso en condiciones de interoperabilidad, considerando el acceso a un tipo de infraestructura u otra forma de instalación a la que los rivales necesitan ingresar para competir. Ello es importante para el derecho a la portabilidad de datos en tanto que, como se verá posteriormente, requiere de la colaboración de los agentes en el mercado digital para que se puedan portar los datos en formatos reutilizables y garantizar que ejecutarlo sea técnicamente posible, entre responsables del tratamiento.

En el caso de Estados Unidos, Graef, Wahyuningtyas y Valcke (2015) comentan que es de aplicación la doctrina de las facilidades esenciales. Esta tiene su origen, específicamente, en el caso Estados Unidos vs. la Asociación de Ferrocarriles de la Terminal de St. Louis[150], bajo la Sección 2 de la Ley Sherman. Se enfoca en la negativa de una empresa dominante a dar acceso a un tipo de

[149] Algunos autores como Crémer, de Montjoye, y Schweitzer (2019) indican, para el mercado económico europeo y su Digital Single Market [único mercado digital], que facilitar el acceso a losdatos, se debe abordar, entre otras áreas, también desde el derecho a la competencia con respecto aempresas que ostentan poder de mercado o de datos:

- Es difícil estimar los efectos de prácticas específicas en el bienestar del consumidor, pero dadas las tendencias de concentración de plataformas y altas barreras de entrada, se requiere de una presunción refutable de anticompetitividad, siendo responsabilidad de la plataforma dominante demostrar que su práctica en juego aporta suficientes ganancias de eficiencia compensatoria.
- Además, las plataformas actúan como reguladores de las interacciones que albergan, por lo que, si son dominantes, deben garantizar lo hacen de manera procompetitiva.
- Las plataformas dominantes deben estar sujetas al deber de garantizar la interoperabildad con los proveedores de servicios complementarios; para ello, las API, interoperabilidad de protocolos y datos, resultan idóneas.

[150] Para mayor información ver: Estados Unidos vs. la Asociación de Ferrocarriles de la Terminal de St. Louis, 224 EEUU 383 (1912).

infraestructura u otra forma de instalación a la que los rivales necesitan acceder para competir. Ha sido aplicada en la Unión Europea y otros países, incluyendo el Perú, aunque con matices distintos en cada caso.

No obstante, en las últimas décadas la Corte Suprema de los Estados Unidos de América ha limitado, considerablemente, el ámbito de aplicación de dicha doctrina en la sentencia "Verizon Communications vs. Law Offices of Curtis V. Trinko, LLP (Trinko), 540 U.S. 398 (2004)" (Graef, Wahyuningtyas & Valcke, 2015, p. 9). En esta sentencia se juzgó que, para ordenar acceso, deberá verificarse lo siguiente:

> [T]he applicable test consists of two prongs: (1) there has to be a pre-existing voluntary course of dealing, and (2) the monopolist must be willing to sacrifice short-term profits in order to achieve an anticompetitive end. These conditions were not met in Trinko in the view of the Supreme Court considering that the monopolist at issue had not voluntarily entered into a course of dealing with its rivals [La prueba aplicable consta de dos aspectos: (1) debe haber un curso voluntario de negociación preexistente y (2) el monopolista debe estar dispuesto a sacrificar ganancias a corto plazo para lograr un fin anticompetitivo. Estas condiciones no se cumplieron en Trinko en opinión de la Corte Suprema al considerar que el monopolista en cuestión no había entró en un curso de trato con sus rivales] (p. 11).

Así, CERRE (2020) indica que, en el sector digital, son interesantes dos casos estadounidenses descritos por el mismo patrón: una pequeña empresa fue confiando en los datos de una plataforma digital más grande para proporcionar servicios de análisis de datos y, luego, se cortó el acceso.

El primer caso, PeopleBrowsr analizó los datos de Twitter para vender información sobre las reacciones de los clientes a los productos o sobre personas influyentes de este medio hasta que decidió que ya no se podría acceder a sus datos directamente, sino que deberían comprarse a revendedores de datos certificados. A raíz de una denuncia de PeopleBrowsr, el Tribunal de Distrito

Norte de California de los Estados Unidos de América (2012) ordenó, con medidas cautelares, que Twitter debía seguir proporcionando sus datos directamente. Determinó que "Twitter's removal lacked an objectively reasonable basis for seeking removal [la eliminación de Twitter carecía de una base objetivamente razonable para buscar la eliminación]"; no obstante, las partes resolvieron el caso y decidieron que, después de un período de transición, PeopleBrowsr obtendría los datos de los revendedores de datos certificados[151](CERRE, 2020).

Segundo, hiQ, mediante *web scraping*[152], analizó los datos públicos disponibles de LinkedIn para proporcionar información sobre aquellos usuarios que estaban en búsqueda de trabajo, hasta que limitó el acceso a estos datos por medios legales y técnicos, porque quería proporcionar servicios similares por sí mismo. Tras una denuncia de hiQ ante el Tribunal de Apelaciones del Noveno Circuito de los Estados Unidos de América, se ordenó a LinkedIn que reanudara el suministro de sus datos[153]. Posteriormente, la Corte Suprema anuló la decisión y remitió el caso para una revisión adicional. En esta segunda decisión, como defensa ante la Corte Suprema, LinkedIn alegó, entre otros argumentos, que permitir dicha práctica ponía en riesgo los datos personales y amenazaba la privacidad de sus usuarios[154] (CERRE, 2020).

---

[151] Para mayor información ver: People-Browsr, Inc. et al v. Twitter Inc. (People-Browsr), N°C-12- 6120 EMC (N.D. Cal. Mar. 6, 2013).

[152] Es una técnica utilizada mediante programas de software para extraer información de sitios web, esdecir, bots programados para examinar bases de datos e información y, muchos de ellos, totalmente personalizables. Se usan para diversas finalidades, en motores de búsqueda para rastrear un sitio, analizar su contenido y clasificarlo; para sitios de comparación de precios que implementan *bots* con el fin de obtener automáticamente precios y descripciones de productos para sitios web de vendedores aliados; o, en compañías de investigación de mercado que lo utilizan para extraer datos de foros y redes sociales (Antevenio, 2019).

[153] Para mayor información ver: https://law.justia.com/cases/federal/appellate-courts/ca9/17- 16783/17-16783-2019-09-09.html

[154] Para mayor información ver: https://www.reuters.com/technology/us-supreme-court-revives- linkedin-bid-shield-personal-data-2021-06-14/

Por otro lado, en la Unión Europea, se aplica la doctrina de las facilidades esenciales, pero con matices diferentes y más amplios. Está recogida como estándar legal para imponer el acceso en la Comunicación de la Comisión Europea (2009) denominada "Orientaciones sobre las prioridades de control de la Comisión en su aplicación del artículo 82º del Tratado constitutivo de la Unión Europea [actualmente 102º del Tratado para el Funcionamiento de la Unión Europea] a la conducta excluyente abusiva de las empresas dominantes", que indica lo siguiente:

> El concepto de denegación de suministro abarca una amplia gama de prácticas, tales como la denegación de suministro de productos a clientes nuevos o existentes, la denegación de concesión de licencias sobre derechos de propiedad intelectual, lo que incluye, cuando la licencia sea necesaria, la información sobre interfaces, o la denegación de concesión de acceso a una instalación esencial o a una red (párrafo 78).
>
> La Comisión considerará que el control de estas prácticas es prioritario siempre que concurran todas las siguientes circunstancias cumulativas (párrafo 81):
>
> - La denegación se refiera a un producto o servicio objetivamente necesario para poder competir con eficacia en un mercado descendente.
> - Sea probable que la denegación dé lugar a la eliminación de la competencia efectiva en el mercado descendente[155].
> - Sea probable que la denegación redunde en perjuicio de los consumidores.

Así, hay dos casos en los que, gracias a esta doctrina, se determinó que prevalece el bienestar de la competencia al brindar acceso a competidores a la infraestructura (entendida como los datos interoperables necesarios), incluso pese a la existencia de derechos de propiedad intelectual:

[155] Es el mercado derivado o secundario, en una fase posterior del producto o servicio analizado.

Primero, el caso IMS Health vs. NDC Health[156], la primera recopilaba información de ventas farmacéuticas de mayoristas en Alemania. Los estructuró con la denominada estructura de ladrillos de 1860, vinculada al sistema postal alemán de códigos; y, luego, proporcionó informes de ventas a dichas empresas farmacéuticas. IMS-Health tenía un derecho de propiedad intelectual sobre esa estructura, por lo que, cuando NDC-Health trató de competir en ventas farmacéuticas con la generación de posteriores informes, el primero se negó a otorgarle una licencia a los mismos (CERRE, 2020).

La quinta sala del Tribunal de Justicia Europeo declaró como elementos para determinar si la estructura protegida es indispensable para la comercialización de estudios de esta naturaleza al "grado de participación de los usuarios en el desarrollo de esa estructura y el esfuerzo, en particular, en cuanto al coste, que los usuarios potenciales deberían realizar para poder comprar estudios sobre las ventas regionales de productos farmacéuticos presentados sobre la base de una estructura alternativa" (pp. I-5087). Concluyó lo siguiente:

> La negativa de una empresa, que ocupa una posición dominante y que es titular de un derecho de propiedad intelectual sobre una estructura de segmentos indispensable para la presentación de datos sobre las ventas regionales de productos farmacéuticos en un Estado miembro, a otorgar una licencia para la utilización de esta estructura a otra empresa, que desea asimismo suministrar tales datos en el mismo Estado miembro, constituye un abuso de posición dominante en el sentido del artículo 82 CE siempre que concurran los siguientes requisitos (pp. I-5088):
>
> - La empresa que ha solicitado la licencia pretenda ofrecer, en el mercado del suministro de datos de que se trata, productos o servicios nuevos que el titular del derecho de propiedad intelectual no ofrece y

[156] Para mayor información, ver: https://curia.europa.eu/juris/showPdf.jsf;jsessionid=51B247696D406C6BF3863FBC3B97CC7B?text=&docid=48679&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=22434766

para los cuales existe una demanda potencial por parte de los consumidores.

- La negativa no esté justificada por consideraciones objetivas.
- La negativa pueda reservar a la empresa titular del derecho de propiedad intelectual el mercado del suministro de datos sobre ventas de productos farmacéuticos en el Estado miembro de que se trate, excluyendo toda competencia sobre este.

La importancia de dicho caso es que para calificar a la estructura de segmentos protegida por derechos de autor como indispensable, se determinó que esta se había convertido en un estándar en el sector, como producto de la posición de dominio ostentada. Por ello, la negativa de otorgar una licencia a tales derechos de propiedad intelectual constituía un abuso de su posición de dominio.

Begoña (2014), en el caso Microsoft vs. Sun Microsystems, relata que la primera le negó a la segunda el proporcionarle la información y la tecnología necesarias para la interoperabilidad de sus sistemas operativos Windows en servidores de grupos de trabajo para ordenadores personales clientes. También, se denunció la realización de contratos vinculados al exigir al comprador que adquiera el Windows Media Player. El Tribunal de Primera Instancia (2004) resolvió ordenar a Microsoft:

> [P]resentar una propuesta dirigida al establecimiento de un mecanismo que ha de incluir la designación de un mandatario independiente revestido de la potestad de acceder, con independencia de la Comisión, a la asistencia, a la información, a los documentos, a los locales y a los empleados de Microsoft, así como al «código fuente» de los productos pertinentes de Microsoft.

Begoña (2014) señala que fue la primera vez que el Tribunal de Justicia Europeo sentó la importancia de la interoperabilidad para el sector de las TIC, en tanto que la información interoperable demostró ser "indispensable en los mismos términos que en el caso IMS Health vs. NDC Health, es decir, el propietario de una

información protegida por derechos de propiedad intelectual[157] que se ha podido convertir en una norma del sector (estándar *de facto)*" (Begoña, 2014, p. 290). Asimismo, se determinó que "la negativa del titular a negociar puede tener como consecuencia la obstrucción a la innovación en el sector del software" (Begoña, 2014, p. 290).

Por su parte, CERRE (2020) aborda tres (3) condiciones para aplicar la doctrina de las facilidades esenciales para determinar en qué casos, el responsable del tratamiento podría verse obligado a conceder el acceso a sus datos tratados, es decir, a licenciar sus derechos de propiedad intelectual[158]:

- Sobre la indispensabilidad de los datos: si se solicitara acceso a datos sin procesar (*raw data*), CERRE (2020) señala que en principio la amplia disponibilidad y ausencia de rivalidad de estos no los hace indispensables, como ha concluido la Comisión Europea en varios casos de fusiones; sin embargo, en casos, su recopilación podría estar sujeta a barreras legales, técnicas y económicas volviéndolos indispensables[159].

[157] El autor hace la salvedad de que no queda claro si lo obligado a divulgar es, en estricto, información protegida por derechos de propiedad intelectual (derechos de autor) o, en su lugar, un secreto empresarial como consecuencia del abuso de la posición de dominio determinado. Este indica que el análisis de la interoperabilidad informática parte de la normativa de propiedad intelectual que abarca, únicamente, programas de ordenar. Por ello, "es posible afirmar que las interfaces informáticas (al menos las especificaciones) estén fuera del ámbito de protección del derecho de autor sobre el programa de ordenador" (Begoña, 2014, p. 292). Segundo, la autoridad podría haber catalogado tal negativa como un abuso del ejercicio de sus derechos de exclusiva, pero "fue interpretada en sentido amplio, como la obstaculización a la aparición de un nuevo producto, porque limitaba el desarrollo técnico en perjuicio de los consumidores" (Begoña, 2014, p. 293).

[158] Para un mayor análisis y relación, se sugiere tener presente lo expresado en la sección 2.2. y 2.2.1, sobre la cadena de valor de los datos y las particularidades del mercado de datos digital.

[159] Como ejemplos a ello, CERRE (2020) comenta que la Comisión Europea encontró en el contexto del caso de Google AdSense, que este servicio tenía una cuota de mercado de más del 90%, en 2016sobre el mercado de búsqueda general en toda la Unión Europea. Igualmente, la Oficina Federal delCartel de Alemania descubrió que Facebook tenía participación de mercado de redes sociales de más del 95% (con respecto a los usuarios activos diarios), en Alemania en diciembre de 2018 (CERRE, 2020).

Si se solicitara acceso a la estructura de los datos, la indispensabilidad implicará determinar si la misma información (o conocimiento) está disponible en el mercado o podría ser construida por una empresa con el mismo tamaño. Es igualmente un problema empírico, pero la estructuración de datos puede conllevar efectos de red importantes y convertirse en un estándar industrial de facto como en el caso IMS Health vs. NDC Health.

Finalmente, el acceso podría ser conjuntamente a datos ya estructurados, es decir, a los datos recopilados y a su estructura, combinando las dos evaluaciones previas.

- Eliminación de la competencia en el mercado descendente: es complejo en los datos, pues su propietario puede negarse a compartirlos con una empresa que todavía no es su competidor, porque planearía ingresar al mercado descendente (el llamado apalancamiento ofensivo futuro o *future ofensive leverage*[160]) o porque teme que, en algún modo, interrumpa su negocio (apalancamiento defensivo o *defensive leverage*). Por lo expuesto en secciones anteriores, el mercado descendente no siempre se conoce o existe, pudiendo tratarse de un competidor en un mercado futuro aún no definido. De acuerdo a Drexl, los datos se recopilan para un propósito, pero pueden resultar en propósitos y sectores muy diferentes (como se cita en CERRE 2020) La evolución en industrias digitales es rápida e incierta y hay paranoia sobre la próxima innovación disruptiva.

- Nuevos productos y daños al consumidor: CERRE (2020) considera que la Comisión Europea integra esta condición en una evaluación más general del daño al consumidor al incorporar las expectativas (futuras) sobre productos

[160] Herrero (2006) señala que la teoría del apalancamiento o *leverage theory* surgió en los Estados Unidos, pero encuentra su paralelo o equivalente en el sistema europeo, en la doctrina del abuso enmercados conexos. Implica que "determinadas prácticas empresariales son explicadas -o utilizadas- como instrumento de extensión del poder de monopolio de un mercado a otro" (Herrero, 2006, p. 366). Una empresa con poder en un mercado determinado se sirve de determinadas prácticas, a modo de palanca, a fin de obtener un poder económico nuevo en un mercado distinto al de la partida(Herrero, 2006).

o servicios que todavía no se brindan y cómo impactarían en el bienestar del consumidor si se restringe la competencia. Para ello, debe determinarse si los datos estarán protegidos por derechos de propiedad intelectual, que dependerá, entre otros, del nivel de la cadena de valor en el que se requiera acceso[161]. Si existe protección de la propiedad intelectual, debe determinarse si el producto del solicitante es suficientemente nuevo o, al menos, mejorado en comparación con los del propietario de los datos. Es decir, examinar si para los consumidores las probables consecuencias negativas de no compartir datos superan, con el tiempo, a aquellas de imponer el intercambio de datos.

Dicho ello, en el plano nacional, la doctrina de las facilidades esenciales también ha tenido cierta acogida y hasta aplicación, aunque no ha estado exenta de críticas.

Diez Canseco (2012) menciona "que un determinado activo califique como facilidad esencial se requeriría la contrastación clara y concurrente de los siguientes requisitos" (p. 68):

- Que sea esencial[162] o de acceso indispensable para que la competidora desarrolle su actividad en un determinado mercado relevante.

- No pueda ser duplicado o replicado y su impedimento de acceso genere la exclusión de la competencia en el mercado.

[161] CERRE (2020) comenta que, igual que Drexl (2016), duda de que este sea el caso, ya que consideraque la generación de nueva información, producto del intercambio de datos, a menudo, no es lo suficientemente innovadora para justificar una licencia obligatoria del derecho de propiedad intelectual.

[162] Para el caso de la esencialidad, el autor cita el ejemplo de una línea ferrovial: aparte de lo costoso (no duplicable), no puede construirse una en el mismo lugar donde ya hay otra.

- Claro exceso de capacidad a efectos de que el acceso concedido a la competidora no menoscabe el uso que la facilidad le estaba brindando a la propietaria, es decir, poseer características de un "bien público".

- Debe concederle a la propietaria una posición de dominio de un monopolio natural (presupuesto de la duplicidad[163]).

El autor señala que una adecuada clasificación de facilidad esencial brindaría principios más claros sobre cuándo una empresa puede negarse a contratar con sus competidores y reduce la limitada predictibilidad y ambigüedad. Además, superaría los problemas de monitoreo de la fijación de precios y/o condiciones de contratación. Esto permitiría señalar, preliminarmente, que este es un remedio más idóneo para ser aplicado por las agencias regulatorias, cortes o agencias de competencia Diez Canseco (2012).

Como se advirtió, en los artículos 10.2º y 10.3º del T.U.O. de la LRCA (2019) disponen que el abuso de la posición de dominio se materializa en conductas exclusorias que afectan a competidores reales o potenciales; y, el negarse injustificadamente a satisfacer demandas de compra o adquisición, o a aceptar ofertas de venta o prestación, de bienes o servicios o aquellas conductas que impidan o dificulten el acceso o permanencia de competidores actuales o potenciales en el mercado por razones diferentes a la eficiencia económica.

Además, entre las facultades de la Comisión y el Tribunal en segunda instancia, está el dictar con ajuste a la intensidad, proporcionalidad y necesidades del daño que se pretenda evitar "la medida cautelar innovativa o no innovativa, genérica o específica, que considere pertinente (…) que contribuyan a preservar la competencia afectada y evitar el daño que pudieran causar las conductas a que el procedimiento se refiere" (artículo 23.2º, T.U.O. de la LRCA, 2019). Así como, medidas correctivas "[d]e acuerdo con las circunstancias, la obligación de

[163] Siguiendo el mismo ejemplo de duplicidad, alega lo irracional y costoso que sería duplicar la facilidad.

contratar, inclusive bajo determinadas condiciones" (artículo 49º, T.U.O. de la LRCA, 2019).

Ello demuestra lo siguiente que señala Diez Canseco (2012):

> [En sede nacional, no se hace] mención expresa a la doctrina de las facilidades esenciales, sino solamente a la teoría de la negativa injustificada a contratar, como un supuesto de abuso de posición de dominio, que en todo caso podría admitir supuestos de negativa a contratar en infraestructuras que se considerasen como facilidad esencial (p. 87).

Por su parte, Tovar (2009) precisa que una facilidad esencial hace referencia a "aquel activo necesario para que los competidores realicen sus actividades. Este debe ser no duplicable por el competidor, no solo por la imposibilidad física o jurídica, sino por la impracticalidad económica" (Tovar, 2009, pp. 346-347). La autora critica la ambigüedad de dicha teoría al pretender "dar acceso aún sin afectar la competencia" (Tovar, 2009, p. 355).

Ahora, se aprecia que jurisprudencialmente la aplicación de la teoría de facilidades esenciales "no ha brindado mayores luces sobre su correcta determinación[164], a fin de saber cuándo se está frente a una facilidad esencial" (Diez Canseco, 2012, p. 93), lo que ha acentuado lo "complejo y confuso que puede llegar a ser" su aplicación (Diez Canseco, 2012, p. 93).

Referencialmente, pues escapa del objeto de esta investigación, en los sectores regulados[165], como las competencias del Organismo Supervisor de

---

[164] La jurisprudencia del INDECOPI es escasa. Resaltan algunos casos como Aero Continente S.A. contra el Banco de Crédito del Perú (Resolución N°870-2002/TDC-INDECOPI) y Cab Cable S.A.contra Electrocentro S.A. (Resolución N°869-2002/TDC-INDECOPI).

[165] En vía regulatoría, Kresalja y Quintana (2005) indican que "el sistema legal peruano también incluye regulación ex ante que define expresamente como facilidades esenciales determinadas infraestructuras y/o recursos" (p. 79), en sectores regulados como telecomunicaciones o infraestructura de transporte donde "la definición de instalaciones o facilidades esenciales otorga a

Inversión Privada en Telecomunicaciones [OSIPTEL][166] y Organismo Supervisor de la Inversión en Energía y Minería [OSINERGMIN][167], se han observado problemas similares a los encontrados tanto en el INDECOPI como en el ámbito internacional. En dichos sectores se ha introducido esta doctrina determinando *ex ante* qué bienes calificarán como una facilidad esencial para efectos su aplicación; por lo que en la práctica ha servido de "herramienta de regulación por la cual los organismos reguladores (OSIPTEL y OSITRAN) tratan de delimitar su aplicación" (Diez Canseco, 2012, p. 93). No obstante, varios autores como Diez Canseco (2012) critican "algunas carencias conceptuales" (p.93) en su contenido y su aplicación por parte de tales organismos a cargo .

Además, Tovar (2009) aclara que, en los marcos regulatorios sectoriales, se identifican las facilidades esenciales y, en torno a ellas, se establece un régimen de acceso obligatorio, por lo que "en caso de negativa del titular a dar acceso a los competidores, no se aplicará la legislación de competencia para ordenar el acceso sino la propia regulación, que contiene sanciones para casos de incumplimiento" (p. 359). Esto da poco espacio a la aplicación del derecho a la competencia, en tanto que es supletorio.

Con todo, Tovar (2009) es enfática al considerar que, ante el INDECOPI, la doctrina de las facilidades esenciales ha aportado ambigüedad y dificultades, por lo que sugiere su descarte en el derecho a la competencia nacional a efectos de

terceros el derecho de solicitar (…) un mandato de interconexión o de acceso, respectivamente, en caso de no llegar a un acuerdo satisfactorio con la empresa que controla dichos recursos" (p. 80).

166 Kresalja y Quintana (2005) mencionan que la regulación de telecomunicaciones "contempla un listado de recursos y servicios calificado como instalaciones esenciales para efectos de la interconexión de redes, tales como la terminación, de llamadas, la conmutación y señalización de llamadas, los servicios de facturación y cobranza, entre otros" (pp. 79-80).

167 En la regulación de infraestructura de transporte de uso público, Kresalja y Quintana (2005) comentan que son facilidades esenciales en las que debe garantizarse el acceso de terceros operadores de servicios sobre los siguientes, entendidos como infraestructuras necesarias: "en aeropuertos, (…) la pista de aterrizaje, la rampa o los puentes de embarque; en puertos (…) la pozade maniobras y rada interior, los muelles y amarraderos, etcétera; similar enumeración se hace paralas carreteras y las vías férreas" (p. 80).

evitar que se vuelva un organismo regulador. Asimismo, recibe el concepto de facilidad esencial, pero debiéndose "cuidad de calificar como tales aquellos activos realmente esenciales para competir, de modo que no se termine eliminando el incentivo para invertir, producir e innovar" (p. 361).

Como se aprecia, más allá de los casos comentados en sede nacional que reflejan la aceptación y aplicación limitada a algunos sectores, reconociéndose ciertos bienes o infraestructura como facilidades esenciales, no se ha advertido algún caso específico en el que se haya discutido si el acceso a una estructura de datos o los datos en sí mismos califican como como una facilidad esencial.

Puede concluirse anticipadamente que, como señalan Krämer y Wolfahrt (2017), el acceso a los datos de otras empresas pareciera estar sujeto a altas barreras legales, económicas y técnicas. Por ello, debe examinarse a fondo bajo qué condiciones previas, nivel de detalle o granularidad y calidad en el acceso a los datos brutos (abiertos) sería útil implementar regulación para promover la innovación y contrarrestar la posible concentración de poder de mercado sin arriesgar la protección de los datos de los titulares de los datos personales y consumidores/usuarios, como de las empresas responsables del tratamiento que ostentan derechos.

La doctrina de las facilidades esenciales fue inicialmente concebida para infraestructuras u otras instalaciones a las que competidores necesitan acceder para competir en mercados descendentes. No obstante, solo internacionalmente (Estados Unidos y la Unión Europea), se ha aplicado en mercados digitales, reconociendo a los datos y su estructura como indispensables. Una empresa con posición dominante puede terminar generando un estándar de facto, en un sector particular, como IMS Health vs. NDC Health o Microsoft vs. Sun Microsystems. Además, en dichos contextos la interoperabilidad también resulta ser una herramienta necesaria para garantizar el acceso adecuado.

Su aplicación no ha sido uniforme incluso dentro de un mismo sector. Ello, probablemente, debido al amplio margen existente para determinar condiciones como la indispensabilidad, eliminación de la competencia efectiva en el mercado

y el posible efecto negativo en los consumidores. Además, debe resaltarse que debido a que el probable producto o servicio futuro a ofrecerse es, en estricto, uno futuro; por ende, resulta difícil analizar un mercado aún no verificable o no se conocen sus particularidades con certeza. Finalmente, ya que es un mercado futuro o potencial en el que el responsable del tratamiento que se niega a otorgar acceso pretendería ingresar, debe considerarse que este, actualmente, tampoco proporciona un producto o servicio en competencia directa a la otra parte. Todo lo anterior eleva las posibilidades de errores anticompetenciales en la aplicación de esta doctrina.

Adicionalmente, el pretender establecer la obligación de otorgar acceso bajo esta doctrina, al menos desde el derecho a la competencia (no en sectores regulados), implica una excepción vía *ex post* que, si bien sí prevalecería ante derechos de exclusividad, se analiza caso por caso. Es decir, no es una medida inmediata y podría tardar en llegar o no hacerlo, si resulta ser el criterio de la autoridad a cargo.

El enfoque abordado con esta doctrina ha sido, en su mayoría, en niveles de la cadena de valor más elevados y casi ningún ejemplo sobre datos brutos (salvo en Twitter vs. People Browsr o hiQ vs. LinkedIn en Estados Unidos). Debe advertirse que es en estos primeros eslabones, sobre todo en el de recolección y organización, donde es más plausible resulte aplicable el régimen de protección de datos personales, al identificar o hacer identificable a sus titulares la data en cuestión. A medida que se asciende, se va formulando el conocimiento de las empresas y se va perdiendo la prevalencia de los derechos del titular de los datos personales a favor de derechos de propiedad intelectual y/u otros de exclusividad del responsable del tratamiento.

Por tanto, cabe la posibilidad que, al calificar como datos personales, se incorpore una arista más, es decir, que prime (como una negativa justificada) el impedir el acceso o divulgaciones a terceros que no cuentan con el consentimiento del titular de los datos personales y como parte de las medidas técnicas, legales y organizativas de seguridad y confidencialidad. Si bien se resolverían problemas como la concentración, generando mejores condiciones para los consumidores al

fomentarse la innovación; no se garantiza que el bienestar de consumidores aumente como consecuencia de disminuirs los efectos de red directos e indirectos existente, es decir, al efecto *lock-in* [encerrar consumidores] y a la incapacidad de hacer *multi-homing*. Además, implementar dichas medidas apartarían la atención de los datos personales como centro de gravedad o protección. Peor aún, se ha mostrado como las preocupaciones sobre protección de datos personales de los usuarios y su privacidad resulta ser un motivo relevante para evitar conceder el acceso en múltiples ocasiones.

Con todo, no debe obviarse que el acceso puede abordarse desde solicitudes de otras empresas en el mercado y usuarios sobre sus datos (Krämer & Wolfahrt, 2017). Por ello, todavía queda analizar cómo garantizar el acceso desde los datos personales y su estructura a fin de permitir su reutilización.

2.3.6 Posibles efectos de la portabilidad de datos en la competencia digital

De acuerdo a Monopolkommission, el acceso a los datos puede ser la base de distorsiones competitivas, si una empresa dominante restringe su acceso (como se cita en Krämer & Wolfahrt, 2017).

Así, la Comisión Europea (2020a) ha señalado recientemente, a la luz de los dos (2) años de transcurrida la aplicación del RGPDP (2016), lo siguiente:

> [L]a privacidad se convierte en un importante parámetro competitivo que los particulares tienen cada vez más en cuenta al elegir sus servicios (…). La introducción del derecho a la portabilidad de los datos tiene el potencial de reducir los obstáculos al acceso de empresas que ofrecen servicios innovadores y favorables en términos de protección de datos. Deberían supervisarse los efectos de un uso potencialmente más amplio de este derecho en el mercado en distintos sectores.

La Comisión Europea (2020a) no niega que "ocasionan a las empresas unos costes inherentes", pues la implementación del derecho a la portabilidad de datos personales generaría costos a cada empresa digital y a cada sector. Por ello, la

portabilidad de datos también tiene una fuerte implicancia en la competencia, así lo manifestó Joaquín Almunia, en el 2012, entonces vicepresidente de la Comisión Europea, responsable de la Política de Competencia:

> [U]sers should be able to move their personal data from one company to another without hassle and undue costs. I believe that a healthy competitive environment in these markets requires that consumers can easily and cheaply transfer the data they uploaded in a service onto another service (…) retention of these data should not serve as barriers to switching. Customers should not be locked into a particular company just because they once trusted them with their content [los usuarios deben poder trasladar sus datos personales de una empresa a otra sin problemas y sin costes indebidos. Creo que un entorno competitivo saludable en estos mercados requiere que los consumidores puedan transferir de manera fácil y económica los datos que cargaron en un servicio a otro servicio (…) la retención de estos datos no debería representar una barrera para el cambio. Los clientes no deben estar encerrados en una empresa en particular solo porque, alguna vez, confiaron en ellos con su contenido]" (Almunia, 2012).

Pero ¿hasta qué punto puede argumentarse o, si es posible, comprobarse que los efectos de la portabilidad de datos personales serían positivos en el mercado, de tal forma que los costos de implementación son compensados (o hasta superados) por los beneficios en la competencia? ¿Existe evidencia empírica, ya sea jurídica o económica, al respecto? El siguiente paso es analizar si la portabilidad de datos aumentaría la competitividad del mercado digital, en tanto sirviera para combatir aquellos efectos negativos (y de qué forma) descritos en secciones anteriores:

- *Multi-homing*: se había adelantado que, el permitir a los consumidores utilizar varios servicios al mismo tiempo y, por ende, considerar que con ello se reduce el riesgo de quedar encerrados en un solo servicio, es falaz. Como Banda (2017) señala, que los usuarios tengan la posibilidad de descargar más aplicaciones y portar sus datos personales, no significa necesariamente que todos sus amigos y familiares los seguirán. Por ello, el

multi-homing, quizá, reduzca los costos de cambio, pero aún los efectos de la red persisten si los usuarios prefieren a una determinada empresa (p. 12).

- Costos de cambio, barreras de entrada y bienestar del consumidor: los costos de transacción y cambio inciden en que cuando se evalúan dos servicios, la diferencia en la utilidad esperada debe al menos exceder al costo de cambio para decidir cambiarse. CERRE (2020) comenta que los consumidores no cambian de un servicio digital porque evitan los costos detransacción de volver a otorgar, sobre todo, grandes cantidades de datos porun período prolongado. Por ello, servicios cuya calidad dependa más de la personalización, serán más propensos a costos de cambio, es decir, tanto los datos proporcionados voluntariamente[168] como los observados[169] constituyen un costo de cambio.

  Por ello, reducir costos de cambio, permitiendo que los datos voluntarios y, según la legislación, los observados, estén disponibles en un "formato estructurado, de uso común y legible por máquina" transmitirlos al nuevo proveedor, puede beneficiar del bienestar del consumidor (CERRE 2020). Así, las *kill zones* o fuertes barreras de entrada podrían ser aminoradas[170]. No obstante, CERRE (2020) y Wohlfarth (2019) advierten que este derecho podría también devenir en efectos secundarios como menos incentivos para economizar el uso de datos. Esto es algo contrario al principio de

[168] Como miles de "me gusta" a canciones en un servicio de transmisión de música en línea.

[169] Siguiendo con el ejemplo, se puede haber grabado qué canciones se escucharon realmente, con qué frecuencia se reprodujo cada canción, durante cuánto tiempo y a qué hora del día. Al igual que los datos proporcionados voluntariamente, pueden ser una entrada muy útil para el próximo servicio.

[170] Mcleod (2020) comenta que las empresas de tecnología más grandes del mundo son tan dominantesque pueden aplastar fácilmente a la competencia con tácticas depredadoras o comprando cualquier amenaza potencial antes de que sean suficientemente grandes como para convertirse en un retador. Lo que es más difícil de rastrear son las adquisiciones menores que nunca aparecen en titulares, pero sacando empresas del mercado antes de que sean relevantes, por lo que la "zona de muerte" no recibe tanta atención como debería. Tal comportamiento anticompetitivo sofoca la innovación y otorga libertad para construir modelos de negocio en torno a la monetización de la información privada.

minimización de datos personales o proporcionalidad, que reduce el bienestar del consumidor por disminuir su privacidad.

Sobre esa posibilidad, Lam y Liu (2020) creen que podría alentar a los titulares de los datos personales a revelar más datos al responsable del tratamiento porque estarían menos preocupados por los costos de cambio. Sin embargo, los autores mencionan que, si revelan más datos, se crearía un mayor efecto de red en el análisis de datos fortaleciendo la posición competitiva frente a nuevos participantes. Krämer y Stüdlein (2019) también consideran que la introducción de este derecho beneficiaría a antiguos clientes del operador establecido, especialmente, a aquellos que se cambian al nuevo proveedor al reducir los costos de cambio y aumentaría la competencia, pero no a los nuevos consumidores porque la posición competitiva del proveedor nuevo se fortalecería rápidamente y, sin portabilidad, este habría competido desesperadamente por nuevos clientes con ofertas interesantes.

- Efectos de red: son omnipresentes en los mercados digitales. A menudo, los servicios están diseñados para incorporar efectos de red directos e indirectos (CERRE, 2020); estos crean un problema de coordinación en el valor del servicio que depende directa o indirectamente de cuántos otros lo estén usando y una situación de bloqueo, porque cambiar de proveedor solo parecerá razonable si todos cambian al mismo tiempo. Como menciona Banda (2017), la portabilidad de los datos no alivia este tipo de bloqueo ni coordinación[171]. Para ello, se requeriría cierta interoperabilidad en los servicios desde la fase del protocolo[172], tal como Crémer, de Montjoye y

[171] En una red social, si se llevara sus datos no se podría interactuar con usuarios de la red anterior.

[172] Incluso, algunos autores promueven la portabilidad de gráficos sociales como una forma de interoperabilidad de protocolos para superar los efectos de red del lado del usuario comparable a la interconexión como en la portabilidad numérica de las redes de telecomunicaciones, en tanto el número de teléfono celular pertenece al cliente y no al proveedor. Por ello, cada consumidor debería poseer todas las conexiones digitales que crea. Así, se iniciaría una sesión en un competidor de cualquier servicio y redirigir instantáneamente todos los mensajes de nuestros amigos de, por ejemplo, Facebook a MyBook (Zingales y Rolnik, 2017). Por su lado, Gans (2018) indica que su

Schweitzer (2019). Ello permitiría que los servicios interoperen hasta un grado en el que los usuarios puedan interactuar, aunque estén en diferentes redes, como en las telecomunicaciones que pueden comunicarse sin importar el operador contratado.

Por su parte, Gans (2018) propone que, a diferencia de Europa y otros países, para suplir los efectos de red en Estados Unidos de América, se opte por la portabilidad de la identidad. Esta implica que los usuarios tengan derecho a su identidad y verificación si cambian de plataforma digital para optar por que todos los mensajes se les reenvíen en dicha nueva red, debido a que los usuarios ya estaban enviando mensajes a una persona con una identidad verificada (p. 13). La identidad debe persistir junto con los permisos que establecen de quién recibir mensajes y a quién enviarlos, así dejarán atrás solo los algoritmos y servicios de la plataforma, pero no sus contactos.

Además, para mitigar el problema de los costos de cambio a los usuarios Gans (2018) propone que las plataformas permitan a los usuarios trasladar su identidad para que las comunicaciones y el contenido que se pretende compartir con otros usuarios puedan enviarse entre plataformas de manera no discriminatoria; los usuarios sean alertados cuando sus mensajes se envíen a otras redes y podrán optar por no recibirlos en cada plataforma; las plataformas asuman los costos de la portabilidad de la identidad, pero elijan la tecnología mediante la cual se ejerce; y, se comience con las redes sociales antes de otros mercados (pp. 5-6).

Sin embargo, exigir la interoperabilidad, desde la fase de protocolo, más allá de la portabilidad de datos, tendría otras implicancias, como la necesidad de supervisión regulatoria. Esto sucede, por ejemplo, en telecomunicaciones. Con ello, también se generaría un mayor riesgo de

propuesta sobre portabilidad de identidad" (p.17) es distinta, pues sí da detalles de su propuesta, proponiendo que se transfiera la identidad verificada de una persona, mientras que los permisos para comunicarse con esa identidad persistirán y podrán modificarse (Gans, 2018).

barreras debido a la necesidad de permanecer dentro de mayores estándares de interoperabilidad, limitándose la posibilidad de entrada y de innovar. Autores, como CERRE (2020), Crémer, de Montjoye y Schweitzer (2019) consideran que, en todo caso, podría ser justificado solo en algunas plataformas o aplicaciones como redes sociales o mensajes de texto, donde los beneficios de la interoperabilidad, probablemente, superen el riesgo de reducir la innovación y competencia; no obstante, la implementación de una medida de tales magnitudes resultaría controversial y probablemente generaría posiciones en contra, sobre todo, desde los actores civiles que se verían directamente afectados u obligados con dicha medida.

Finalmente, CERRE (2020) indica que la provisión de datos a los competidores se iniciaría por los consumidores y solo sus datos. Sería muy diferente a una solicitud de acceso por otra empresa, por ejemplo, bajo la doctrina de las facilidades esenciales que podría también otorgar datos de entrada (anonimizados) sobre un gran número de usuarios. Es poco probable que todos los usuarios comiencen una transferencia de sus datos y, más bien, bajo la portabilidad, el conjunto transferido sería más detallado sobresujetos específicos, pero menos representativo en el conjunto de usuarios. Por ello, la utilidad de los competidores dependería de un análisis específicode cada contexto y del grado en que los consumidores porten sus datos.

- Incentivos a la innovación: actualmente, sin algún tipo de acceso obligatorio a datos, las empresas intensivas en datos los controlan para obtener beneficios económicos, ya sea vendiendo su acceso o utilizándolos para mejorar productos o servicios y obtener una ventaja competitiva. Esto crea un incentivo económico para invertir tanto en la recopilación y en análisis de datos, como en innovación a servicios derivados. Por ello, CERRE (2020) indica que perder control sobre esos datos, económicamente podría inducir a un problema de atraso, pues los beneficios económicos serían inciertos, reduciendo la inversión y la innovación.

De acuerdo con Arrow (1962)[173], en un entorno monopolístico con altas barreras de entrada (por efectos de red o costos de cambio u otros), los incentivos a la innovación tienden a ser bajos porque innovar no brinda una ventaja competitiva. En la visión schumpeteriana, los mercados con alta competencia tienen bajos incentivos a la innovación porque las rentas se eliminarían rápidamente y no se daría la escalabilidad suficiente[174]. Por ello, los incentivos a la innovación más altos se dan en condiciones oligopólicas (Aghion et al.2005), como en los mercados digitales. CERRE (2020)destaca que los incentivos a la innovación serán altos si un mercado aún nose ha inclinado por un agente dominante y hay cierta competencia o, si a pesar de existir un monopolio de facto, las barreras de entrada fueran tan bajas que el titular tuviera que defender constantemente su posición con innovación[175].

[173] Wilson (2019), la Comisionada de la Comisión Federal de Comercio de Estados Unidos de América, indica que existe una versión moderna y adaptada de Arrow, la cual defiende la proposición de que los mercados atomistas son siempre más innovadores que los concentrados. Pero Arrow (1962), sostiene que "el incentivo para innovar es menor en condiciones de monopolio que en condiciones de competencia" (pp. 7-8, 1962). Ello, por supuesto, indicando dos salvedades obviadas en el presente: (i) se disfruta de importantes barreras de entrada y solo el monopolio tiene la capacidad de inventar; y, (ii) una situación de monopolio temporal, como una situación previa de innovación en la que no hay impedimento de entrada a nuevas empresas con innovaciones propias, es más competitiva que una monopolística *per se*. Por ello, la mayoría de las industrias son más pro-competitivas que monopolísticas y más innovadoras que su hipotético monopolio puro (Arrow, 1962 citado por Wilson, 2019).

[174] Wilson (2019) sostiene que, para Schumpeter, el rastro de la innovación se atribuye a las grandes empresas y no a la competencia comparativamente libre. Históricamente, las grandes empresas pueden haber tenido más que ver con la creación del nivel de vida que con afectarlo. Schumpeter (2006) define al proceso de innovación como un "ventarrón de la destrucción creativa" (p. 83). La historia del aparato productivo de cualquier industria está incesantemente revolucionando la estructura económica desde adentro, destruyendo incesantemente lo "viejo" para crear algo "nuevo" (Schumpeter, 2006). Bourne (2019) también indica que tal proceso de innovación de las empresas consiste básicamente en innovar para capturar consumidores, logrando participación de mercado y siendo finalmente usurpado por otro nuevo competidor en el mercado.

[175] Bourne (2019), igual que Schumpeter, cuestiona la existencia de regulación estatal para controlar la presencia monopolística. En el siglo pasado, grandes empresas fueron etiquetadas como monopolios perpetuos, basándose en un razonamiento económico similar al de empresas de tecnología actuales.

CERRE (2020) señala que, en la práctica, las innovaciones en datos inferidos (análisis de datos) se basan en la entrada de datos brutos (observados y ofrecidos voluntariamente). Hay un círculo vicioso porque las innovaciones a nivel de análisis de datos facilitan la innovación a nivel de servicio, incluso en diferentes rubros. Se requieren suficientes datos brutos para empezar a operar servicios, lo cual es imposible si no hay clientes. Este es el problema del arranque en frio[176]; por ello, si clientes prueban el servicio, aunque sea una vez, se ofrecerán más recomendaciones útiles[177].

Así, algunos autores son optimistas en que el derecho a la portabilidad de datos permitirá solucionar este problema. Serán los mismos usuarios quienes porten sus datos personales a nuevos servicios, ya sea a competidores directos o potenciales en mercados secundarios, sin necesidad de recurrir a otros mecanismos como la doctrina de las facilidades esenciales u otros para promover la innovación.

Por su parte, Graef, Husovec y Purtova (2017) tienen una visión más escéptica. Ellos cuestionan si el tipo de control que apunta a un reúso más intensivo a nivel económico o de mercado para fomentar la innovación de datos y servicios pertenece a la protección de datos y sus raíces en la

Sin embargo, casos históricos como Great Atlantic and Pacific Tea Company, Myspace, Nokia, Kodak, iTunes de Apple, Internet Explorer de Microsoft y más muestran que ninguna aseguró un dominio continuo. Sus cuotas de mercado se desintegraron, ante nuevos productos y empresas innovadores, como teorizó Schumpeter. Deberíamos ser escépticos sobre predicciones de un poder monopolístico arraigado para Amazon, Google, Facebook, Apple y Microsoft. Por ello, basar la política antimonopolio hacia superar el dominio de unas empresas o legislar para evitar daños futuros altamente especulativos, califican como "una tontería".

[176] Para mayor información ver: https://towardsdatascience.com/the-cold-start-problem-with-artificial-intelligence-49938ed3f612

[177] Para proporcionar buenos resultados, un sistema de recomendación o predicciones de algoritmos debe estar alimentado con suficientes datos de usuario observados y/o proporcionadosvoluntariamente para hallar similitudes y derivarlas en recomendaciones o predicciones.

privacidad, y si la ley de protección de datos es el lugar más adecuado para abordar todos estos problemas económicos relacionados con los datos.

Curiosamente, CERRE (2020) indica que el sector en el que se evidencia que el derecho a la portabilidad ha impactado positivamente al promover la innovación, fomentar la entrada de nuevos competidores, mejorar el bienestar de los consumidores y el control de los titulares de los datos personales al tener acceso a (y posibilidad de elegir) mejores condiciones de privacidad; es el *Open Banking*[178]. Si bien había competencia previa entre los bancos, la aparición de nuevos servicios financieros (*fintech*), se impulsó tras la disponibilidad de API que hicieron posible la portabilidad continua de datos, y el desarrollo de múltiples servicios y aplicaciones complementarios.

Por ello, no existe evidencia certera sobre si es necesario tomar medidas drásticas en el mercado digital para evitar que sectores monopólicos u oligopólicos continúen siéndolo, más cuando definir un mercado relevante es complejo y relativo, ya que muchas empresas muestran presencias multilaterales. Tampoco es claro si las barreras de entrada lo son. Más allá de Schumpeter, en el sector digital, la innovación es clave para mantener el dominio y elevados estándares de calidad.

Por ello, si bien Graef, Husovec y Purtova (2017) tienen razón al señalar que pretender atribuir mayores propósitos al derecho a la portabilidad no resulta adecuado, estos autores cuestionan que el extrapolar y generalizar que mediante la reutilización estandarizada y el intercambio de datos personales se va a lograr incidir -ya sea de forma general o concreta- en la competencia para fomentar nuevos competidores directos o indirectos en mercados secundarios, contribuir a lidiar con los efectos de red, al *multi-homing* y reducir las barreras de entrada coadyuvando con problemas como el "arranque en frio"; no son los motivos principales por los que se permita o fomente que el titular de los datos personales tenga mayor control sobre sus datos personales. Por ello, no debe perderse de vista

178 Para mayores detalles ver: https://www.openbanking.org.uk/what-is-open-banking/

que los datos personales aluden al derecho de autodeterminación informativa y manifiestan la personalidad.

El Open Data Institute [ODI] (2018) ha indicado que los potenciables beneficios de la portabilidad de datos personales al mercado digital son transversales. Los enlistó de la siguiente manera: competitividad, al cambiar entre proveedores de productos y servicios iguales o similares; complementariedad, al permitir transferir datos personales a terceros que brindan productos o servicios que, complementarios al uso original de los datos, generan y comparten valor-conocimiento entre diferentes tipos de actores[179]; no relacionado, además de respaldar productos y servicios competitivos y complementarios entre sí, puede permitir usos no relacionados como organizaciones de confianza con fines de investigación, entre otros.

Exposito-Rosso, Cao, Piquet y Medjaoui (s.f.) indican que la regulación a la portabilidad de datos, permitirá aumentar los datos y su valor al poder agruparlos y accederlos fácilmente. La diferencia competitiva efectiva estará en cómo aprovecharlos; la persona y sus datos ya no son el producto, lo será el servicio adaptado cada vez más a la persona[180]. Además, tiene un valor social que trae beneficios más amplios que los únicamente económicos ya citados, como una infraestructura social mejorada a los usuarios; se promoverá el pluralismo y la diversidad de los medios, al haber más incentivos para que fuentes de noticias ofrezcan noticias de calidad en lugar de buscar maximizar la atención del usuario y los ingresos publicitarios con desinformación y discursos de odio; y, existirán incentivos para ofrecer mayor privacidad, compitiendo en términos de calidad de la privacidad y en mejorar la portabilidad de los datos (Exposito-Rosso, Cao, Piquet & Medjaoui, s.f.).

179 Como transferir datos médicos de hospitales, un reloj inteligente al buscar un seguro de salud o data de propiedades constantemente alquiladas para las aseguradoras de bienes inmuebles.

180 Esta postura es similar a la de CERRE (2021).

2.4 Consideraciones técnicas para la portabilidad de datos personales

Como señala Ctrl-Shift (2018), en su reporte al Departamento Digital, Cultura, Medios y Deporte del Reino Unido, el RGPDP (2016) solo crea un derecho a la portabilidad de datos, mas no lo habilita ni crea las estructuras para respaldar la generación de valor a partir de dicha portabilidad. Los nuevos derechos que las personas tienen sobre sus datos presentan también potenciales nuevos peligros para las personas y las organizaciones con las que interactúan. Por ello, Krämer y Wolfahrt (2017) indican que debe preverse un sentido técnico porque los datos en el mercado digital se recuperan con mayor frecuencia, a través de las API, lo cual tiene implicancias en las dificultades de lectura ulterior.

La calidad y el nivel de acceso a los datos juega un papel crucial. Estos influyen en aspectos como si los datos se proporcionan inmediatamente o con demora, cuántos datos se pueden recuperar por solicitud, y qué interfaces y formatos de datos son proporcionados por el proveedor de servicios. Como se ha planteado, el acceso a datos es factible en varios grados de granularidad, desde datos sin procesar (como entradas de usuario directas y no estructuradas) hasta perfiles de usuario ya atribuidos (Krämer & Wolfahrt, 2017). Para analizar los aspectos técnicos de la portabilidad de datos y el intercambio de datos, seanalizará la forma en que se almacenan los datos personales; cómo se implementan las funciones de exportación o transferencia de datos, los estándaresy los sistemas; y, qué otras posibilidades y/o innovaciones existen para tales fines.

Primero, los modelos y formatos de datos utilizados para representar, almacenar e intercambiar datos dependerán, en gran medida, del tipo de datos utilizados. CERRE (2021) clasifica dichas variedades de formatos en estructurados[181], que siguen un formato tabular rígido, con un conjunto

[181] Estos se intercambian típicamente como archivos CSV (un formato de datos simple para datos tabulares), archivos SQL (un estándar para sistemas de bases de datos relacionales) o archivos de hoja de cálculo, como OpenDocument o Office Open XML de Microsoft. Sin embargo, ninguno de estos formatos es ideal para el intercambio de datos porque no están completamente estandarizados. No hay una forma específica de describir la codificación de caracteres utilizada o que incluyan características más allá del alcance de la representación de los datos estructurados.

predefinido de campos; semiestructurados[182], que siguen una forma jerárquica, mezclando contenido estructurado y texto potencialmente no estructurado, con una variedad de atributos de datos que no necesitan definirse con anticipación; y, los no estructurados, que no encajan en los anteriores y comprenden texto sin formato en lenguaje natural, datos multimedia (imágenes, sonidos, videos) y otros datos binarios arbitrarios.

Como primer paso, para entender la información contenida en los datos, debe conocerse la sintaxis (formato de archivo) y el esquema de los datos, es decir, qué campos y atributos de datos existen y qué restricciones deben respetarse sobre los valores de los datos. Por ejemplo, algunos formatos de archivos, como CSV y las hojas de cálculo, no ofrecen ninguna capacidad de descripción del esquema, salvo el dar nombres a las columnas. Por ello, la metadata, en ciertos archivos, juega un papel más crucial que en otros, al describir cómo debe entenderse el esquema empleado. Tema aparte es que sobre la metadata también se requieren consensos para su escritura y lectura (CERRE, 2021).

Segundo paso, los datos deben interpretarse con respecto a una semántica específica. Esta da significado a los campos y atributos de datos, a lo que se denomina dialecto o vocabulario de datos. Como se comentó, para algunas áreas del análisis de datos, ya existen dialectos estandarizados, como GPX, que es un estándar *de facto* para intercambiar trazos GPS o Dublin Core, que es otro estándar *de facto*, a un vocabulario de datos para describir obras digitales y físicas.

---

[182] Ejemplos de estos formatos son XML, diseñado como un formato de intercambio de datos simple para información semiestructurada. Como alternativa surgió JSON, que se basa en el lenguaje de programación JavaScript con la ventaja de ser menos detallado y que te permite transferir la información más fácilmente al subirla a otros servicios; y, RDF (marco de descripción de recursos) sobre XML para representar información en forma de gráficos semánticos que vincula un concepto semántico (el sujeto) a otro concepto semántico o valor de datos (el objeto), a través de un predicado semántico que indica la relación entre ambos. Ambos formatos no son excluyentes, en tanto RDF se creó, originalmente, en 1999 como un estándar sobre XML para codificar metadatos. Para mayor información ver: https://github.com/JoshData/rdfabout/blob/gh-pages/intro-to-rdf.md#Introducing%20RDF.
Finalmente, HTML tiene la ventaja de que permite abrirse como una página web en cualquier navegador.

Sin embargo, si no hay dialecto previo suelen haber varios otros *ad-hoc* compilados por cada responsable del tratamiento. Esto genera que, ante un intercambio de datos, no haya homogeneidad, sino heterogeneidad de esquema, debiéndose incurrir en el gasto de transformar los datos de un esquema al otro, con mapeos de esquemas desde la fuente al destino (CERRE, 2021).

Esto grafica por qué la transferencia y posterior uso de datos personales por terceros responsables del tratamiento en el mercado carecen de una adecuada estandarización a nivel sintáctico y semántico, con múltiples limitaciones para la transferencia y posterior reutilización de los datos. Gal y Rubinfeld (2019) identifican tres (3) obstáculos principales que reducen los incentivos a transferir y reutilizar datos por parte de terceros[183]:

- Incertidumbres en los metadatos: al estar estos relacionados con la semántica de los datos o con la precisión con la que se registraron, pueden limitar la capacidad de comprensión o conducir a suposiciones incorrectas[184].

- Obstáculos para la transformación de datos, que aumentan los costos y dificultan combinar los datos disponibles en conjuntos de datos coherentes, pueden ser difíciles de integrar o incluso generar la necesidad de reorganizar los datos en una estructura u organización interna diferente.

- Falta de datos: en caso no se recopilaran algunos datos necesarios, el hacerlo posteriormente, puede ser imposible o muy costoso.

[183] Los autores, en base a la Comisión Europea, señalan que fusionar diferentes conjuntos de datos y hacerlos interoperables es una de las actividades más intensivas en recursos para quienes hacen uso de esos datos que, increíblemente, dentro de la misma cadena de valor, los conjuntos de datos, rara vez, son interoperables por defecto.

[184] Los autores ponen el ejemplo del incidente del Mars Climate Orbiter, diseñado para estudiar el clima marciano. En septiembre de 1999, la nave se acercó demasiado al planeta y se quemó en la atmósfera. La falla resultó del uso de dos estándares diferentes en una base de datos y la combinación de datos de las dos fuentes dio un cálculo erróneo que originó el accidente (Gal y Rubinfeld, 2019).

Por ello, los beneficios de la estandarización de datos al mercado de datos son múltiples. Para Gal y Rubinfeld (2019), la estandarización de datos implica establecer estándares relacionados con la cadena de valor de los datos, ya sea sobre sus atributos, terminología, estructura, organización, almacenamiento (ubicación), uso y protocolos para su portabilidad. También, los autores señalan que la estandarización de datos puede reducir potencialmente todos los obstáculos, anteriormente mencionados, en el uso de datos por terceros; aumentar los incentivos para la recopilación y posterior tratamiento; y, generar cantidades mayores, más valiosas, accesibles y con menos costos para su portabilidad (Gal y Rubinfeld, 2019).

Así, las herramientas para transferencias de datos más utilizadas son las API, que son protocolos de computadora que definen cómo los componentes de software se comunican entre sí. Las API facilitan el flujo de datos al describir los tipos de estos que se pueden recuperar, cómo hacerlo y el formato en el que se compartirán. Estas también pueden incluir a los metadatos asociados. Son importantes, pues describen los atributos o la semántica de los datos y permiten a los usuarios interpretar el significado y la importancia de diferentes puntos de los datos. Sin embargo, si bien en algunas industrias existe un consenso con respecto a qué API se usan, en muchas otras, no lo hay. Tampoco, se conoce si son preferibles las abiertas y/o estandarizadas. Adviértase que las API no resuelven completamente los tres (3) obstáculos principales señalados (Gal y Rubinfeld, 2019).

A continuación, se analizarán los dos (2) modelos técnicos posibles que existen en la práctica comercial y técnica para cumplir el derecho a la portabilidad de datos: la exportación de datos, donde el titular de los datos personales recibe los datos del responsable; y, la transferencia de datos, que se da directamente entre responsables del tratamiento, a solicitud previa del titular de datos personales.

2.4.1 Exportación de datos personales

CERRE (2021) distingue hasta tres (3) formas en las que se le puede permitir al titular de los datos personales, exportar sus propios datos.

- Asincrónicamente: tras un periodo de tiempo considerable desde la solicitud del titular de los datos personales, el responsable del tratamiento pone a disposición los datos personales solicitados para que sean descargados.

- Por extracción: de forma casi inmediata, el responsable del tratamiento proporciona los datos personales solicitados a su titular.

- Por solicitud anticipada: si es posible que el titular de los datos personales manifieste anticipadamente su intención de portar sus datos personales para que, tan pronto como se traten nuevos datos personales, el responsable del tratamiento se los envía o pone a su disposición para descargarlos.

Para ahondar en la práctica comercial, se revisará qué mecanismos técnicos, en esta modalidad, han implementado algunas de las empresas digitales más conocidas a nivel mundial. Así, como advierte CERRE (2021), Facebook, Google, Microsoft y Twitter se enfocan en un modo de exportación de datos asincrónico con capacidades de consulta generalmente muy limitadas, que, en su mayoría, permiten seleccionar aplicaciones o categorías específicas para ejercer la exportación y, casi siempre, no se ofrece garantía sobre el retraso al tiempo estimado de atención:

- Google (s.f.) indica que “[s]egún la cantidad de datos que tengas en tu cuenta, este proceso puede tardar desde unos minutos hasta varios días. Lo más habitual es obtener el enlace el mismo día en que lo solicitas". Asimismo, permite la opción de “Exportaciones Programadas”, mediante la

opción "[c]rea automáticamente un archivo con los datos seleccionados cada dos meses durante un año"[185].

- Twitter (2021) indica que "[i]t may take a few days for us to prepare the download of your Twitter archive [podría tomarnos unos cuantos días preparer la descarga de tu archivo de Twitter]"[186].

- Instagram (2021) puede tardar "hasta 48 horas en recopilarte y enviarte estos datos, y solo puedes solicitar un archivo cada cuatro días". Tampoco, permite una descarga parcial de los datos personales segregando en base a criterios, como si lo ofrecen otras redes sociales como Facebook. Además, "es posible que algunos datos que hayas eliminado se almacenen de forma temporal por motivos de seguridad y protección, pero no aparecerán cuando accedas a tus datos o los descargues" (Instagram, 2021).

- Facebook (2021) indica que sí es posible seleccionar la totalidad de datos o los tipos de datos personales (que están extensamente segregados)[187], intervalos de fechas que interesen y el formato en que se desean exportar:

> Puedes descargar una copia de tu información de Facebook cuando quieras. Puedes descargarla en su totalidad o seleccionar solo los tipos de datos e intervalos de fechas que te interesen. Tienes la opción de recibir esta información en formato HTML, que permite una lectura sencilla, o en formato JSON, que facilita la importación mediante otro servicio. La descarga de tu información es un proceso protegido con contraseña al que solo tú tienes acceso. Una vez creada la copia, estará disponible para su descarga durante algunos días. Si quieres consultar tu información sin descargarla, puedes acceder a tu información cuando quieras.

---

185 Para mayor información ver: https://support.google.com/accounts/answer/3024190#zippy=%2Cexportaciones-programadas

186 Para mayor información ver: https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive

187 Para mayor información ver: https://www.facebook.com/dyi/?referrer=yfi_settings

Además, el resultado del modo de exportación de datos asíncronos, suele ser, en la mayoría de los casos, un archivo ZIP, es decir, un comprimido de varios archivos, salvo para Google, que también permite archivos en formato TGZ. Los formatos más comunes de dichos archivos son JSON, para información semiestructurada; formatos de archivos multimedia para imágenes o audio; HTML, que permite ser visualizado por cualquier navegador web; y, otros como dialectos XML y CSV.

Cabe resaltar que la manera en que se brinda el servicio de exportación, en las tres modalidades anteriores, es mediante API. Pese a que estas, por lo general, usan formatos comunes, como JSON o CSV, todavía sigue existiendo poca estandarización y una gran variedad de dialectos entre una empresa, incluso dentro de un mismo sector. Esto podría ser resuelto, ya sea con estándares de facto (consensos) o ciertas disposiciones legales que no resulten restrictivas.

Por otro lado, debe ponderarse si todos los datos personales deberían ser exportados bajo la misma forma o modalidad, es decir, de forma asincrónica. Lo anterior se debe analizar porque hay casos con gran cantidad de datos a exportar que puede demorar tiempos irrazonables que van en contra del espíritu del derecho de la portabilidad de datos personales que es inmediato y fácil (características propias del entorno digital), ya que no tienen que reingresar o generar nuevamente dicha data. Este es el caso de Instagram que demora cuarenta y ocho (48) horas para atender la solicitud o, en su defecto, con la legislación del RGDP que le puede otorgar hasta un (1) mes, susceptible de extensión.

Así, podrían explorarse otras opciones (y/o conjugadas), con el derecho de acceso, que vuelvan la exportación lo más inmediata posible. Algunas plataformas permiten acceder primero a la data y, tras visualizar de forma disgregada, se puede tener una idea de qué intervalos o criterios se desean portar. Es el caso de Facebook que permite acceder a tu información por categorías[188]. Así, el usuario puede, preliminarmente, disgregar la información que requiere y, con ello, ir a la

[188] Para mayor información ver: https://www.facebook.com/your_information

sección de descargar tu información y solicitar los criterios que son de su interés. Sea que ambas secciones estén separadas o, que dicha solicitud pudiera hacerse en la misma página web inmediatamente, el tener la facilidad de visualizar el contenido exacto que se obtendría de forma previa, permite al usuario discernir con anticipación si verdaderamente desea o no portar su totalidad.

Finalmente, otra opción útil es la posibilidad de exportación de datos por solicitud anticipada a efectos de que, como Google ofrece, pueda decidirse, con anticipación, qué datos personales se desearán portar (de forma continua) cada cierto tiempo. Sus beneficios son que permiten disminuir la carga de los archivos a ser portados gracias a la periodicidad y otorga una mayor visibilidad a los titulares de los datos personales como usuarios la plataforma.

2.4.2 Transferencia de datos personales directa

CERRE (2021) comenta que, para una transferencia de datos entre titulares, también se emplean API que permiten, igual que en el modo anterior, la exportación de datos, principalmente, por extracción, como respuesta casi inmediata a los datos personales solicitados; y, ocasionalmente, por solicitud anticipada. No obstante, la transferencia de datos directa entre titulares conlleva particularidades que pueden ser agrupadas dentro de estas dos (2) modalidades:

- Intercambio directo: los datos se transfieren directamente desde el responsable del tratamiento de los datos personales a otro destinatario designado por el titular de los datos personales, independientemente que la transferencia se inicie por el remitente o destinatario. En cualquier caso, el responsable de los datos personales que inicie la transferencia de datos actúa como un cliente de la API, usando un protocolo de delegación de acceso, que le permitirá obtener un *token* de acceso para demostrar que ha sido autorizado por el interesado y, con ello, cumplir con medidas de seguridad y confidencialidad adecuadas. Asimismo, suele emplearse el cifrado o la encriptación en la transferencia y la asignación desde el esquema de origen al de destino para mayor seguridad, entre otras medidas.

Por ende, se requiere que los responsables del tratamiento de origen y de destino implementen la capacidad de transferencia de datos y la asignación desde el esquema de origen al de destino, pero solo se necesita una única API en todo el procedimiento de transferencia. Así, el titular de los datos personales debería otorgar primordialmente (o únicamente) su consentimiento al responsable del tratamiento de los datos personales que accederá a la API del otro a efectos de concretar la transferencia.

- Intercambio a través de un tercero: los datos personales se transfieren desde el responsable del tratamiento de origen a un sistema de terceros, siendo los más comunes en el mercado los llamados PIMS. Dicho tercero actuaría como el cliente de la API ante el responsable de los datos personales de origen. Seguidamente, el sistema de terceros utilizará nuevamente otra API del responsable del tratamiento de los datos personales, que es el destinatario y quién a su vez proporcionará acceso de escritura para transferir o recibir los datos personales y asignará a los mismos el esquema de destino.

  Es decir, la transferencia de datos y las asignaciones de esquemas, si bien son manejadas por el sistema del tercero que se designe, requieren de dos (2) API: una para el acceso de lectura, en el responsable del tratamiento de origen; y, otra, para el acceso de escritura en el responsable del tratamiento de destino. Por ello, el consentimiento (o solicitud) del titular de los datos personales deberá comprender el sistema del tercero para acceder ambas API en origen y destino.

Con todo, CERRE (2021) advierte que en ambos casos existe un problema de confianza, ya que el permiso asociado a los *tokens* de acceso, rara vez, es lo suficientemente detallado como para que el titular de los datos personales pueda estar seguro de que el único uso que se hará de ellos es para la tarea de transferencia de datos. Un ejemplo es que la validez en el tiempo puede extenderse más allá del tiempo necesario para la transferencia de datos. Una solución es la propuesta en el *Data Transfer Project* de Google que será abordada más adelante,

pero se adelanta que propone el uso de *tokens* con una única validez y expirando automáticamente, una vez verificada la transferencia.

2.4.3 Analizando las particularidades de las API

Además de lo mencionado sobre las API, CERRE (2021) ratifica que esta interfaz técnica permite acceder a los datos utilizados por programas, sobre todo softwares de terceros, lo que permite introducir aplicaciones novedosas a los datos. Permiten especificar qué tipo de acceso tendrán los softwares de terceros sobre los datos de cierto programa específico manteniendo la seguridad y el control.

En estricto, las API pueden ser de varios tipos. En este caso, a las que se viene haciendo referencia son las API web, empleadas dentro del entorno en línea. Estas permiten consultar recursos (información) de un servidor en una dirección URL completa que se le denomina *endpoint*. Cada recurso consultado tendrá un identificador uniforme (o único), que se denomina *URI*. A este se le responderá con distintos códigos que indican qué paso con la petición realizada. Sobre las mismas, se detallarán algunos componentes esenciales en la funcionalidad de las API:

- Pueden ser locales, cuando están dentro de un mismo servidor; y, remotas, cuando utilizan distintos servicios web que pueden estar en cualquier punto del mundo. Estas son las más comunes, pues las API web suelen ser diseñadas para interactuar en una red de comunicaciones, es decir, en Internet (Red Hat, s.f.).

- Uso de HTTP y/o HTTPS: al ser una API web, emplean el protocolo de comunicación *Hypertext Transfer Protocol* (HTTP), que permite la transferencia de archivos en la *World Wide Web* o Internet. Ahora, como medida de seguridad, se suele realizar el envío de información prefiriéndose al HTTPS (una versión más segura del anterior) y cuya denominación en español es protocolo seguro de transferencia de hipertexto. Este permite que el flujo de la información, que se envíe en la web, viaje de forma cifrada;

así, en caso de interceptaciones o atacantes, estos no podrán develar el contenido de la información enviada (Edteam, 2019).

- Sobre las arquitecturas para implementarlas, las dos (2) más usadas son SOAP, un protocolo simple de acceso a objetos que, si bien inicialmente fue un protocolo más usado que impone reglas integradas, quedó en cierto desuso debido a que "aumentan la complejidad y la sobrecarga, y podría retrasar el tiempo que tardan las páginas en cargarse; sin embargo, estos estándares también ofrecen normas integradas que incluyen la seguridad, la atomicidad, la uniformidad, el aislamiento y la durabilidad" (Red Hat, s.f.).

  Representational State Transfer (REST) o transferencia de Estado Representacional, que, a diferencia del anterior, no posee un estándaroficial, únicamente, especifica ciertos principios arquitectónicos. Ofrece "mayor flexibilidad frente a contextos más nuevos, como el IoT, el desarrollo de aplicaciones móviles y la informática sin servidor" (Red Hat,s.f.). Entre sus pautas están las siguientes: la arquitectura "cliente-servidor"(compuesta por el cliente[189] que hace la solicitud a un recurso por medio delHTTP) y el servidor (quien responde si cumple con las condiciones); sin estado y la capacidad de almacenamiento en memoria caché, pues elcontenido de los clientes no se almacena en el servidor entre las solicitudes, sino que la información sobre el estado de la sesión se queda en el cliente, almacenada en su memoria caché del cliente; el sistema en capas, entanto las interacciones cliente-servidor pueden estar mediadas por capas adicionales que ofrecen funcionalidades adicionales; el uso de mensajes autodescriptivos, en tanto cada mensaje que se devuelve al cliente contiene la información suficiente para describir cómo debe procesarse la información; etc.

[189] Nótese que el cliente es la aplicación web, móvil, de escritorio, para *smart TV*, un dispositivo IoT, etc. o llamado tercero responsable del tratamiento, que quiere acceder al recurso que está protegido,en nombre de alguien (es decir, del titular de los datos personales). Este cliente puede ser una aplicación.

- Los formatos de los recursos entregados por las API, suelen ser tanto JSON, que es el formato más común, pero también se usan otros como XML o incluso el texto plano o escrito (EDteam, 2019).

- Pueden ser públicas o privadas: la primera implica que cualquiera pueda acceder y consultar la información permitida de forma libre, mientras que las privadas requieren una autenticación que suele darse a través de *tokens*, como JWT el cual fue el formato más común en las API REST (EDteam, 2019).

- Es común el uso de especificaciones y protocolos para la asignación de *tokens* de acceso seguro en la identificación, autenticación y autorización de cada usuario, a fin evitar ataques o vulneraciones en la identificación de los clientes al solicitar acceso. También, se suele recurrir a *tokens* con un tiempo de expiración lo más corto posible y *scopes* asignados, que son los permisos para hacer algo dentro de un recurso protegido en nombre de un usuario. Así, existen distintas especificaciones, protocolos de autenticación (verifica la identidad) y protocolos de autorización (verifica el consentimiento otorgado por parte del titular de los datos personales al tercero que desea acceder al recurso), que se utilizan en el entorno API, como OAuth 2.0[190] para la autorización, que es el más usado y se ha convertido en un estándar de facto; sin embargo, también resaltan otros que, a veces, son conjuntamente usados por funcionalidades adicionales como OpenID, OpenID Connect[191] para la autenticación y otros como *"Kantara UMA, Universal Authentication Framework, Universal Second Factor,*

[190] La especificación OAuth 2.0 define un protocolo de delegación que es útil para transmitir decisionesde autorización a través de una red de aplicaciones y API habilitadas para la web. OAuth se utilizaen una amplia variedad de aplicaciones, incluido el suministro de mecanismos para la autenticaciónde usuarios. Esto ha llevado a muchos desarrolladores y proveedores de API a concluir incorrectamente que OAuth es en sí mismo un protocolo de autenticación y a utilizarlo erróneamentecomo tal. Para información ver: https://oauth.net/articles/authentication/

[191] Es un estándar abierto, publicado en 2014, que define una forma interoperable de utilizar OAuth 2.0para realizar la autenticación de clientes. Para mayor información ver: https://openid.net/connect/

Mozilla Persona, Security Assertion Markup Language, Gigya" (Comisión Europea, 2016, p. 10).

2.4.4 Sistemas de gestión de información personal (PIMS)

Adicionalmente, al uso de las API, varios autores han resaltado como algo positivo fomentar el uso de las *Personal Information Management System (PIMS)*[192] o, en español, el Sistema de Gestión de Información Personal. Según CERRE (2021), son un sistema diseñado para permitirle a sus usuarios tener una vista integrada de sus propios datos personales contenidos en otros múltiples servicios proporcionados por plataformas web como correos electrónicos y otros tipos de mensajería, calendarios, contactos, búsquedas web, redes sociales, información de viajes, proyectos laborales y cualquiera que genere información del usuario.

Por ello, su uso no es excluyente con una API; por el contrario, su objetivo es manejar todos los datos personales de un usuario desde un sistema que el usuario controle y confíe; posee, a la fecha, dos (2) modalidades. La primera tiene un enfoque de almacenamiento que permite transferir todos sus datos (personales y no personales) al PIMS para que sean también almacenados localmente. La segunda tiene un enfoque de mediación que mantiene los datos distribuidos en cada plataforma, utilizando una metodología de integración de datos. Esto permite interactuar con todas las fuentes de sus datos, sin necesidad de que sean almacenados localmente. Según CERRE (2021), esta opción es más escalable, pues no requiere tantos recursos de computación ni almacenamiento local como el anterior; no obstante, depende, en gran medida, de la disponibilidad de API lo suficientemente potente para expresar las consultas de los usuarios traducidas de forma interoperable. Esto quiere decir que se requiere una mayor interoperabilidad a nivel de sistema, mientras que la primera opción podría implementarse desde la interoperabilidad a nivel de datos[193].

---

192 Para mayor información de un caso de PIMS que opera en el mercado y cumple con los requerimientos del RGPDP: Para mayor información ver: https://dataguardian.eu/manager/es/

193 CERRE (2021) advierte que, las PIMS podrían permitirle al usuario formular consultas como ¿qué tipo de interacción tuve recientemente con cierta persona? y ¿dónde fueron mis últimos diez viajes

Si bien la transferencia de datos no es la función principal de las PIMS, estas podrían permitir enviar los datos a otros responsables del tratamiento de datos, actuando como un tercero entre el responsable de origen y destino, de forma continua y en cualquier momento. Lo anterior, en tanto su objetivo, es ofrecer una visión completa y actualizada de los datos personales del usuario. Por ello, sería el PIMS quien inicie las llamadas a cada API, controle los *tokens* de acceso e implemente las asignaciones de esquemas. Sin embargo, para todo lo anterior, resulta fundamental que el usuario confíe plenamente en la PIMS elegida, y que cuente con adecuadas medidas de seguridad y confidencialidad.

¿Existen a la fecha PIMS que hayan sido ampliamente adoptadas y, de ser así, qué tan viables de adoptar/implementar son? A la fecha, sí existen distintas iniciativas de PIMS ofrecidas sea por gobiernos o por organizaciones privadas que cuentan con respaldo gubernamental e incluso iniciativas netamente privadas gratuitas y/o en otras modalidades con cobros bajo diversas modalidades, como *freemium*.

En estricto, cada iniciativa tiene sus particularidades en las consideraciones técnicas que usa, pero, de manera general, estas emplean medidas de seguridad de autenticación y autorización, similares a las API. Además, para garantizar la seguridad de sus arquitecturas, existen modelos de PIMS, basados en almacenamiento centralizado de la información en la nube que facilitaría el desarrollo de ofertas de análisis como servicios adicionales que permiten a las PIMS autofinanciarse. También, existen ofertas basadas en modelos descentralizados o distribuidos en la fuente original de recolección con el fin de ofrecer el intercambio de documentos. Un ejemplo de ello es Cozy Cloud[194], que ofrece servicios de nube privada descentralizada y permite implementar una

de negocios y quién me ayudó a planificarlos? Ante dichas preguntas el sistema deberá consultar a los distintos servicios adscritos e integrar la información de ellos. Ejemplos de respuesta a dichas preguntas implicarían vincular una ubicación GPS del usuario con una dirección de algún establecimiento comercial o un lugar mencionado en un correo electrónico u otra mensajería; o, un evento en un calendario con algún evento en una búsqueda web realizada por el usuario.

194 Para mayor información ver: https://cozy.io/es/

PIMS. Otro ejemplo en el mercado es Digi.me[195], que ofrece un PIMS con control detallado sobre qué datos privados se envían a qué controlador de datos.

Sobre las garantías técnicas que eviten el uso de los datos personales más allá del consentimiento del titular, destacan también medidas innovadoras como el diseño de plataformas PIMS, bajo el esquema o tendencia denominada de conocimiento cero. Esta tendencia implica que el proveedor de la plataforma no podrá acceder a los datos personales almacenados en la cuenta del usuario, si este no le otorga su consentimiento para ello.

2.4.5 Otras iniciativas en el mercado

Una iniciativa, a nivel mundial, que puede servir para el cumplimiento del derecho a la portabilidad, que, a su vez, permite empoderar al titular de los datos personales otorgándole control sobre sus datos personales en el entorno digital, son los Personal Data Services (PDS) o, en español, los Servicios de Datos Personales. Dicha tecnología consiste en equipar a un individuo, que será el usuario PDS, con un dispositivo (físico o virtual[196]) que representa un contenedor que proporciona mecanismos técnicos a los usuarios para capturar, almacenar, procesar de acuerdo con las preferencias del usuario, gestionar y controlar la transferencia de datos personales sin procesar y los resultados del análisis u otros cálculos de los datos personales en el dispositivo, así como dar ulterior seguimiento y control a los datos personales entrantes y salientes del dispositivo frente a los distintos servicios o aplicativos web que los requieran (Janssen, et. al., 2020).

Así, su finalidad es empoderar a los usuarios, a través de medios que ponen a las personas en control de sus datos, por ejemplo, al brindar más detalles sobre las aplicaciones que instalan a través de mecanismos que permiten a los usuarios definir qué pueden hacer las aplicaciones con sus datos; brindar niveles más altos

---

195 Para mayor información ver: https://digi.me/get-started/

196 Por ejemplo, la iniciativa Databox prevé un dispositivo físico diseñado para un hogar y uncomponente virtual que es un software almacenado en la nube. Para mayor información ver: https://www.horizon.ac.uk/project/databox/

de transparencia sobre el procesamiento de datos al proporcionar información a los usuarios, a través de varios medios, sobre qué datos desea acceder la aplicación y cómo se procesarán esos datos; y, llevar a cabo procesos de evaluación de riesgos para las aplicaciones que admiten, etc.

Los desarrolladores y/o proveedores de servicios online que requieran realizar tratamientos sobre los datos de un usuario no necesitarán acceso directo, pues estos se realizarán en el dispositivo del usuario, de acuerdo con el consentimiento otorgado y solo sobre un conjunto definido de sus datos. Finalmente, el desarrollador o proveedor del servicio recibiría solo los resultados agregados de cualquier cálculo o tratamiento que, como argumentan los defensores de PDS, podrían ser menos personales, sensibles o invasivos, pero potencialmente más valioso para las empresas.

A la fecha, la tecnología PDS es poco desarrollada, pero está ganando importancia. Hay varias iniciativas en curso en etapas de desarrollo e implementación (Janssen, et. al., 2020). Algunos ejemplos son Dataswift / Hub of All Things[197], Mydex[198], digi.me[199], CitizenMe[200], Databox[201], Solid Project[202], Personium[203], etc.

Otra iniciativa distinta, específicamente desarrollada para cumplir con el derecho a la portabilidad de datos personales en el RGPD, es el *Data Transfer Project* (DTP)[204]. Esta es una iniciativa técnica, lanzada en 2018, por empresas de tecnología como Apple, Facebook, Google, Microsoft y Twitter. Consiste en una

197 Para mayor información ver:

- https://www.dataswift.io/about/about-dataswift
- https://www.hubofallthings.com

198 Para mayor información ver: https://mydex.org

199 Para mayor información ver:https://digi.me/

200 Para mayor información ver: https://citizenme.com

201 Para mayor información ver: https://www.horizon.ac.uk/project/databox/

202 Para mayor información ver: https://inrupt.com/solid/

203 Para mayor información ver: https://personium.io/en/index.html

204 Para mayor información ver: https://datatransferproject.dev/documentation

especificación y plataforma de código abierto para la transferencia de datos, utilizando las API existentes de los servicios o plataformas, entre las que se realizará la transferencia y los mecanismos de autorización para acceder a los datos personales; luego, se utilizan adaptadores específicos del servicio para transferir esos datos personales a un formato común y, después, se recurre a la API del nuevo servicio destinatario para la recepción de los datos[205]. Se dice que este es un proyecto heredado del antiguo proyecto *Data Liberation Front* de Google. Por ello, a la fecha tal empresa es su mayor contribuyente.

Su objetivo es admitir el intercambio directo entre responsables del tratamiento, en los términos del RGPD. A la fecha, se encuentra en desarrollo y no considera ni permite una transferencia continua de datos, sino solo la transferencia masiva a iniciativa del titular de los datos personales que decide transferir sus datos personales de una plataforma a otra. Si bien se han implementado varios conectores de importación y exportación para interactuar con varias plataformas, son pocas las que se han adherido al mismo.

2.4.6 Experiencias técnicas de sectores digitales en la portabilidad de datos personales

La portabilidad de datos personales debe prever la capacidad de transferir datos sin afectar su contenido. Por ello, se requiere cierto grado de interoperabilidad para garantizar, al menos, cierta capacidad de integrar los datos portados al banco de datos personales del receptor. Lo anterior sirve para garantizar su reutilización. Si la combinación de datos de diferentes fuentes, tras ser portados, se vuelve viable, permitirá mejorar el conocimiento que se pueda extraer de los mismos y tendrá efectos económicos positivos en el sector digital y en el mismo titular de los datos personales. Sin embargo, el panorama actual plantea múltiples barreras a la portabilidad (e interoperabilidad requerida) de los datos personales. Por ello, un primer paso es fomentar la interoperabilidad de los datos personales con un acceso continuo, siendo el mecanismo más usado las API privilegiadas con

205 Para mayor información ver: https://datatransferproject.dev/dtp-overview.pdf

autorización previa del titular de los datos personales y, con esto, la estandarización.

En ello, la experiencia de otros mercados, como CERRE (2021) comenta, es que con respecto al RGPDP (2016), la viabilidad técnica de los derechos de portabilidad de datos es mínima y está lejos de ser ideal. De esta manera, solo es posible realizar exportaciones de datos asincrónicas; no hay garantía sobre el retraso entre la solicitud; y, los datos proporcionados en la exportación no siguen ningún estándar específico e incluyen una amplia variedad de modelos de datos, formatos de archivo, esquemas, dialectos, de tal manera que no resultan incompatibles entre un responsable del tratamiento de datos personales y otro, incluso, dentro de un mismo sector. Esto evidencia que los responsables del tratamiento de datos personales no implementan verdaderas facilidades para su intercambio.

Por ello, las capacidades de intercambio de datos se ven obstaculizadas por la heterogeneidad de esquemas y, en general, por la falta de estandarización en distintos niveles. Resulta clave analizar qué estrategias de estandarización resultan deseables, así como considerar sus posibles impactos económicos. Para esto, se ahondará en experiencias regulatorias comparadas, a nivel técnico, anticipando que deben preferirse estándares abiertos y comunes para favorecer la innovación. A su vez, permite la regulación específica de cada sector, pues los estándares de facto que proliferaron pueden diferir totalmente y/o ser innecesarios en otros sectores:

- El caso ejemplar del *Open Banking*, que se inició en el Reino Unido y la "Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) 1093/2010 y se deroga la Directiva 2007/64/CE", indica que el derecho a la portabilidad de los datos tuvo un impacto positivo para promover la innovación y fomentar la entrada de nuevos competidores, mejorando consecuentemente el bienestar de los consumidores y control de los titulares de los datos personales al tener acceso (y posibilidad de elegir) a mejores condiciones de privacidad. Esto

gracias a la aparición de nuevos servicios financieros (*fintech*), mediante la disponibilidad de interfaces comunes basadas en API que hicieron posible la portabilidad continua de datos y el consecuente desarrollo de múltiples servicios y aplicaciones que complementaron los servicios financieros en el mercado.

CERRE (2021) comenta que, en la Unión Europea, la legislación sectorial complementa el derecho de portabilidad del RGPDP (2016), desde la perspectiva B2B (*business to business*, es decir, entre proveedores de servicios), ya que obliga a los bancos, quienes son los responsables del tratamiento iniciales, a permitir la transmisión directa de la información bancaria personal de los titulares de los datos personales a terceros proveedores (por ejemplo, los servicios de iniciación de pagos o servicios de información de cuentas).

Así, con la regulación sectorial bancaria se obliga a los bancos garantizar la viabilidad técnica de esta portabilidad de datos de cuentas financieras en la vía B2B. Por otro lado, fomenta que esta portabilidad sea continua, ya que los interesados pueden solicitar datos personales en cada transacción, facilitada por una API. CERRE (2021) comenta que, posteriormente, la Comisión Europea adoptó normas técnicas de regulación sobre la base de un borrador presentado por entidades de dicho sector privado, imponiendo un estándar abierto, común y seguro para la comunicación entre los proveedores de servicios en el sector bancario.

Por su parte, en el Reino Unido, se llevó a cabo el *Open Banking Programme*, administrado por el *Open Banking Implementation Entity* (OBIE), que es un nuevo organismo independiente que implementó una API abierta y común para acceder a la información de las cuentas de los clientes de los nueve bancos más grandes del país con el fin de incrementar la competencia y la innovación en el sector. La OBIE desarrolló, dentro de un plazo fijo (y corto), estándares de datos de productos que sean técnicos comunes, abiertos y de solo lectura; y estándares bancarios comunes, abiertos de lectura y escritura para el intercambio de datos de transacciones.

Esos estándares garantizan que cualquier comunicación sea segura y se base en el consentimiento de los clientes.

En sede nacional, si bien no existe regulación específica del *Open Banking*, existen iniciativas privadas como "Modelo Perú"[206]. Esta es una interfaz que permite generar procesos de inclusión financiera y un ecosistema de pagos digitales con intermediarios financieros, que dio origen a la billetera electrónica interoperable Bim[207]. La anterior está conformada por más de 30 entidades financieras y emisoras de dinero electrónico y utiliza la tecnología *Ericsson Wallet Platform*, lo que da la opción de realizar transferencias, pagos, compras y obtener información sobre la actividad del usuario en todo tipo de celulares sin necesidad de ser smartphones.

A la fecha, resaltan otras iniciativas como la plataforma Interbank API[208], que contiene publicadas las API para que otras aplicaciones se integren y puedan utilizar los servicios financieros que proporciona el banco. Un ejemplo de ello, son los casos de Rappi Bank y Kambista[209]. Esta última es una *fintech*, dedicada al cambio de divisas en el Perú. Asimismo, existen algunos casos a nivel regional, que cuentan con presencia en el sector financiero peruano como Prometeo[210].

Si bien no hay regulación específica, existen algunas disposiciones que podrían aplicar tangencialmente, como el artículo 21° de la Resolución de la Superintendencia de Banca y Seguros [SBS], N° 504-2021, "Reglamento de Ciberseguridad de la SBS", aplicable a las entidades financieras supervisadas por la SBS, que establece que la implementación de las API, para la provisión de servicios y demás operaciones a través de servicios terceros, deberán cumplir con ciertas medidas, tales como el análisis de

206 Para mayor información ver: https://mibim.pe/archivos/Documento-PDP.pdf

207 Para mayor información ver: https://pagosdigitalesperuanos.pe/#quienes-somos

208 Para mayor información ver: https://developers-dev.digital.interbank.pe/#/docs/api/autorizacion

209 Para mayor información ver: https://alertaeconomica.com/casos-de-open-banking-en-peru/

210 Para mayor información ver: https://prometeoapi.com/

riesgos asociados e implementar medidas de mitigación; la autenticación mutua de los sistemas y usuarios; la autorización de operaciones por parte de los usuarios; el cifrado de datos en almacenamiento o transmisión; las prácticas de desarrollo seguro de API y la revisión de prácticas de codificación segura; el análisis de vulnerabilidades y pruebas de penetración; la seguridad de infraestructura tecnológica que lo soporte; los mecanismos de tolerancia ante fallos y de contingencia; el control de accesos en el entorno de datos, sistemas e infraestructura; y la gestión de incidentes. Asimismo, las especificaciones técnicas de las API utilizadas deben encontrarse documentadas de forma que facilite su auditoría y la implementación necesaria para su uso. Finalmente, se deberá adoptar estándares y marcos de referencia internacionales y, cuando sea factible, mediante acuerdos gremiales o sectoriales.

Por otro lado, la SBS ha declarado que se encuentra realizando estudios asociados a las opciones disponibles para el desarrollo del *Open Banking* en el Perú. Igualmente, el Banco Central de Reserva del Perú (BCRP), dentro de su Reporte de Estabilidad Financiera, de mayo de 2021, se ha pronunciado indicando que la regulación del *Open Banking,* a emitirse, debería especificar, como mínimo, el nivel de detalle de la información del cliente requerido para ser compartida con los terceros autorizados y el uso que se daría a dicha información. Sin embargo, no detalla el tipo de información que debería compartirse; la regulación aplicable para el consentimiento de los usuarios; los estándares de las API; las entidades que estarían bajo el alcance de la norma; ni el plazo de adecuación e implementación de la norma.

- El sector energético, dentro de la Unión Europea, en tanto que mediante el artículo 23° de la "Directiva (UE) 2019/944 sobre normas comunes para el mercado interior de la electricidad y por la que se modifica la Directiva 2012/27/UE", impuso "garantizar el acceso e intercambio de datos eficiente y seguro, así como la protección de los datos y la seguridad de los datos" de los consumidores, incluidos los datos de medición y consumo, así como los datos necesarios para para el cambio de suministrador, la respuesta de

demanda y otros servicios. Así, dicha directiva supone un claro complemento al RGPDP (2016) en el sector energético, al exigir a sus Estados miembros que establezcan un régimen específico para el intercambio de datos de consumidores, el intercambio entre proveedores de electricidad y el reconocimiento de que "[e]l tratamiento de datos personales en el marco de la presente Directiva se llevará a cabo de conformidad con el Reglamento (UE) 2016/679" (apartado tercero del artículo 23º mencionado).

- En normativa del consumidor en la Unión Europea, conforme al artículo 16° de la "Directiva (UE) 2019/770, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales a petición del consumidor", el empresario pondrá a disposición del consumidor, previa petición de este último, contenidos que no sean datos personales y que el consumidor haya facilitado o creado al utilizar los contenidos o servicios digitales suministrados por el empresario sin cargo alguno y sin impedimentos por parte del empresario. Esto se da en un plazo razonable y en un formato utilizado habitualmente y legible electrónicamente. Al igual que en materia de protección de datos personales, en el ámbito del consumidor, también se permite la portabilidad de los datos y aplica a todos los proveedores de contenidos o servicios digitales, pero únicamente otorga al consumidor el derecho a recuperar algunos de sus datos no personales sin permitir la transmisión directa entre dos empresarios. No obstante, la idea subyacente de esta Directiva es permitir que los consumidores recuperen sus datos para, luego, compartirlos con otros comerciantes, garantizando que los consumidores puedan cambiar fácilmente de proveedor de contenido, al reducir los obstáculos legales, técnicos y prácticos, como lo es la imposibilidad de recuperar todos los datos.

- El caso del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, que aplica en relaciones B2B y sobre aquellos datos no personales, prevé en su artículo

6°, que se fomentará y facilitará la elaboración de códigos de conducta autorreguladores a escala de la Unión Europea para contribuir a una economía de datos competitiva, basada en transparencia e interoperabilidad con estándares abiertos que incluyan aspectos como los siguientes:

2.4.1 [M]ejores prácticas para facilitar el cambio de proveedores de servicios y la portabilidad en un formato estructurado, de uso común y de lectura automática, incluidos formatos basados en estándares abiertos cuando lo exija o solicite el proveedor de servicios que reciba los datos.

2.4.2 [R]equisitos de información mínimos, antes de celebrar un contrato de tratamiento de datos relativa a los procedimientos; requisitos técnicos; y, plazos y costes aplicables en caso de que se desee cambiar de proveedor de servicios o transferir sus datos a sus propios sistemas informáticos. [E]nfoques de regímenes de certificación que faciliten la comparación de los productos y servicios de tratamiento, teniendo en cuenta las normas nacionales o internacionales establecidas, que facilitan la comparabilidad de estos productos y servicios que podrán incluir, entre otros, la gestión de la calidad, la gestión de la seguridad de la información, la gestión de la continuidad de negocio y la gestión medioambiental.

- Un ejemplo nacional es la portabilidad numérica en el servicio público móvil y en el servicio de telefonía fija en el Perú, conforme al Texto Único Ordenado del Reglamento de Portabilidad Numérica en el Servicio Público Móvil y el Servicio de Telefonía, aprobado mediante Resolucion de Consejo Directivo Nº 286-2018-CD-OSIPTEL.

  Si bien los números telefónicos (móvil e incluso fijo) pueden constituir datos personales, la relación entre la portabilidad de telecomunicaciones y de datos personales, en el sector digital, difieren sustancialmente. Por esto, aporta pocas referencias prácticas a diferencias de otros sectores que sí son

digitales, pues son dos sectores distintos en los que la materialización de la portabilidad no resulta de una aplicación directamente análoga.

Con dicha precisión, en su artículo 4º, se reconoce la portabilidad numérica como un derecho de todo abonado independientemente de la modalidad contratada. Así, la portabilidad para el servicio público móvil es no geográfica (en todo el territorio del país) y, para el servicio de telefonía fija, es geográfica (solo para el departamento en el que contrató dicho servicio). Ahora bien, sí resultan de utilidad algunas disposiciones normativas que serán ahondados en el capítulo siguiente. Tales consideraciones son (i) la información a ser proporcionada al abonado por el Concesionario receptor en el artículo 5º; (ii) el deber del Concesionario Receptor de verificar la existencia de facilidades técnicas y el plazo de respuesta para ello, debiendo indicarse los motivos del impedimento técnico en caso se deniegue la solicitud de portabilidad al aducir inexistencia de facilidades técnicas para ello; (iv) el deber de información del Concesionario Cedente estipulado en el artículo 7º; y, (v) el criterio de gratuidad para el abonado en el artículo 10º.

- En materia de Gobierno Digital en Perú, el reciente documento de trabajo para el "Diseño de la Estrategia Nacional de Gobierno de Datos Abierto (2021-2026)" busca la ejecución de "una gestión pública eficiente tomando decisiones con base en datos, y que promueva su uso y la interoperabilidad entre el sector público, privado, la academia y sociedad civil", así como impulsar el desarrollo de ecosistemas alrededor de los datos (PCM, 2021).

  Aparte de que propone reconocer a los datos como activos y promover su monetización[211], cabe resaltar que propone en su Eje 1, sobre la Gestión de

[211] Idea reconocida en la presente investigación y empleada como sustento para el reconocimiento del aspecto económico de los datos personales en el sector privado. Ello es razón para considerar que el titular de los datos personales no solo requiere de una esfera de protección de sus datos personales de forma restrictiva con respecto a derechos fundamentales, sino de forma armónica y contemporánea a los intereses económicos, propios del entorno digital en el que interactúa.

Datos, el asegurar la interoperabilidad de los datos, mediante la definición de estándares para la asignación de identificadores de calidad yconsistencia, y la integración de múltiples fuentes para aumentar la credibilidad de los datos y la explotación analítica (PCM, 2021). Para ello,se han propuesto acciones como normalizar e inventariar los identificadoresúnicos[212], en toda la administración pública, sector privado y academia; promover que entidades públicas, privadas y la academia publiquen API con identificadores homologados para interoperar; y, promover la normalización de los datos para el sector público, privado y academia.

Puede observarse que el objetivo estratégico del documento de trabajo, va alineado con la mencionada Gestión del Marco de Interoperabilidad del Estado Peruano, al trazar acciones concretas para asegurar que la interoperabilidad de los datos, entre las entidades públicas y privadas, como la necesidad de contar con API para poder entablar la interoperabilidad necesaria entre las entidades públicas. Además, se consideraron ciertos criterios de estandarización, como lo son los identificadores usados para interoperar los códigos de identificadores únicos estandarizados y elaborar catálogos de metadatos sobre los identificadores únicos estandarizados.

Por ello, las acciones adoptadas en materia de Gobierno Digital y en el presente documento de trabajo son un referente a nivel nacional de las reformas necesarias en la regulación privada. Esto indica la necesidad de emitir una regulación específica para cada sector digital a efectos de permitir el intercambio de datos personales (y no personales), atendiendo a las particularidades de cada industria; por ejemplo, en el documento de

[212] A la fecha, dicho documento de trabajo indica que los Identificadores Únicos son los siguientes: (i) RENIEC, Código Único de Identificación de personas naturales; (ii) MIGRACIONES, Código Único de Identificación de extranjeros; (iii) SUNARP, Número de Partida Registral de personas jurídicas y Número de la placa única nacional de rodaje del vehículo; e, (iv) INEI, Código de ubicación geográfica (UBIGEO), Clasificador de Actividades Económicas, Código de Ocupaciones y Código de Carreras e Instituciones Educativas de Educación Superior y Técnico Productivas, Clasificador Nacional de Programas e Instituciones de Educación Superior Universitaria, Pedagógica, Tecnológica y Técnico Productiva. Para mayor información ver el artículo 72º del Reglamento de la Ley de Gobierno Digital.

trabajo, se menciona que para estandarizar los datos abiertos de geolocalización se debe recurrir a los estándares ISO 3166 o, en el caso de los datos de salud, al estándar internacional HL7.

De igual manera, con respecto a la infraestructura tecnológica necesaria, en el Eje 2, se contempla como Objetivo Estratégico el implementar guías, procesos y estándares tecnológicos que garanticen la interoperabilidad de los datos, sistemas informáticos y plataformas a todo nivel. Todo será materializado con las siguientes acciones: implementar un catálogo de API/WebServices; incorporar estándares ISO a todo nivel; definir las políticas para el intercambio electrónico de homologado y seguro entre las diversas instituciones del país e instituciones externas; e, implementar estándares para el uso e integración de plataformas en la nube (pública, privada, híbrida) que permitan escalamiento.

CAPÍTULO III: ASPECTOS NORMATIVOS PARA LA PORTABILIDAD DE DATOS PERSONALES

3.1 Consideraciones legales para la portabilidad de datos

Al hablar del derecho a la portabilidad de datos personales, en el entorno digital, no se puede olvidar la convergencia de ciertas áreas del derecho en el negocio del mercado de datos: de la competencia (incluyendo proveedores y consumidores digitales), del consumidor (que ayuda a los consumidores como la parte más débil en las transacciones del mercado) y la ley de protección de datos personales (proporcionando control de sus datos personales a los titulares de los mismos). Existe una base en la protección de los derechos fundamentales (como se revisó en la sección 1.4 anterior). Debido a sus diferentes alcances de protección, los cuatro regímenes pueden complementarse entre sí, pero también entrar en conflicto según la forma en que se aborde el intercambio de datos (Crémer, de Montjoye, & Schweitzer, 2019). Por ello, resulta deseable analizar la fórmula del Proyecto Ley (2021), considerando a todos los actores involucrados.

Además, por un tema cronológico, dicho análisis se realizará considerando el estado actual del Proyecto de Ley (2021) que, si bien pasó a archivo y no logró ser debatido ni ser objeto de mayores modificaciones, podría volver a ser presentado en un futuro. Con la salvedad anterior, en la Exposición de Motivos del Proyecto de Ley (2021) se reconoce que el derecho a la portabilidad de los datos personales "se encuentra relacionado al derecho de acceso a la protección de los datos personales" (p. 29), ya que permite recibir los datos que, sobre sí mismo, se hayan proporcionado "y poder transmitirlo a otro responsable o titular" (p.29). Anteriormente, se demostró que la doctrina y la legislación extranjera han sido claramente mayoritarias al establecer que el derecho a la portabilidad, más que relacionarse, subyace al derecho de acceso, siendo una expresión o actualización del inminente fenómeno de digitalización frente a las limitaciones del derecho acceso en entornos digitales. Sin embargo, por motivos de brindar mayor autonomía y promover su implementación, varias legislaciones lo han incorporado como un derecho nuevo.

Por las dos consideraciones anteriores, se discrepa con la fórmula actual del Proyecto de Ley (2021) que pretende incorporar dicho derecho como el artículo 23-Aº, es decir, dentro del artículo 23° de la LPDP (2011), correspondiente al derecho del tratamiento objetivo que es un derecho totalmente distinto al de la portabilidad de datos personales. Lo anterior aunado a que en la misma Exposición de Motivos se prevé que el derecho a la portabilidad es un derecho "relacionado al derecho de acceso (...) ya que permite recibir los datos que sobre sí mismo le haya dado al responsable de tratamiento o titular de banco de datos y poder transmitirlo a otro responsable o titular".

Así, resulta contradictorio que, si el propio Proyecto de Ley (2021) advierte una naturaleza relacionada entre ambos derechos, pretenda finalmente incorporarlo dentro de una sección correspondiente a un derecho totalmente distinto como el derecho al tratamiento objetivo. Por ello, debe ser incluido como un artículo independiente o, al menos, dentro de la sección correspondiente al derecho al acceso, siempre y cuando se haga hincapié que este es independiente al derecho de acceso, pues responde a particularidades regulatorias distintas. Así, se evitarían confusiones por parte de los administrados y de la propia autoridad al momento de ponerlo en práctica.

También se resaltó que su objetivo es empoderar a los titulares de los datos personales, al mejorar su facultad de trasladar, copiar o transmitir datos personales fácilmente de un entorno informático a otro propio o a los de otros responsables del tratamiento, pudiéndose así utilizar o destinar dicha data personal a diversas finalidades. Tal objetivo se encuentra previsto tanto en la autodeterminación informativa, como en el control que debería ejercer el titular de los datos personales, mediante su derecho de acceso. Por ello, son objetivos, en principio, comunes. No obstante, el derecho a la portabilidad de datos personales pretende asegurar su reutilización dentro del entorno digital sin necesidad de tenerse que volver a ingresar los datos, sino solo al ser portada por el propio titular o, de ser técnicamente posible, entre dos responsables del tratamiento. Las personas que hacían uso de su derecho de acceso se veían limitadas por el formato elegido por el responsable del tratamiento para proporcionar la información solicitada, algo

que fue por el Grupo de Trabajo 29 (2016), en la anterior Directiva sobre protección de datos 95/46/CE y todavía apreciable en la legislación peruana.

Por último, al asentar los derechos personales de los individuos y reafirmarse el control del titular de los datos personales sobre sus datos personales, la portabilidad de los datos representa una oportunidad para reequilibrar la relación entre los interesados y los responsables del tratamiento. De ahí se analiza su incidencia en las relaciones de consumo dentro del entorno digital. En esa línea, puede contribuir a la competencia entre los servicios digitales facilitando y promoviendo el cambio de servicio y el uso de datos personales en la industria dentro de los parámetros normativos.

3.2 Análisis regulatorio comparado

En adelante, se destinarán esfuerzos a dar recomendaciones sobre qué esquema normativo y/u orientativo puede ser el más favorable atendiendo a las particularidades económicas, técnicas y legales del derecho a la portabilidad de datos personales, considerando las experiencias de regulación extranjeras.

Así, el RGPDP (2016), mediante el Grupo de Trabajo 29 (2017), indica que el derecho a la portabilidad de datos personales[213] consta de cuatro (4) elementos:

[213] Como se mencionó, el artículo 20º del RGPDP (2016) contiene la siguiente fórmula legislativa:

> 1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
>
> a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
>
> b) el tratamiento se efectúe por medios automatizados.
>
> 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
>
> 3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el

- Derecho a recibir datos personales: implica que el titular de los datos personales tiene derecho a recibir un subconjunto de datos personales que le conciernan sobre el responsable del tratamiento y almacenarlos para un uso personal posterior, ya sea en un dispositivo privado o en una nube privada, sin transmitirlos necesariamente a otro responsable del tratamiento. Por ello, complementa al derecho de acceso, pues ofrece a los interesados una forma sencilla de gestionar y reutilizar por sí mismos sus datos personales.

- Derecho a transmitir datos personales de un responsable del tratamiento a otro responsable del tratamiento: esto a petición del titular de los datos personales y cuando sea técnicamente posible. Proporciona a los interesados la posibilidad de obtener, reutilizar y transmitir a otro proveedor de servicios en el mismo sector (u otro) los datos facilitados. Así, se evita la retención de consumidores y se promueve la innovación, el intercambio y reutilización de datos entre responsables del tratamiento de forma segura y bajo el control del titular de los datos personales.

- Responsabilidad: la portabilidad de los datos garantiza el derecho a recibir los datos personales y a tratarlos conforme a los deseos de su titular. Por ello, el responsable actúa a nombre del titular de los datos personales, pero deberá establecer garantías que aseguren que se actúa a su nombre. Así, los responsables del tratamiento, que responden a solicitudes de portabilidad de datos, no son responsables por el tratamiento que realice el titular de los datos o quien sea el receptor. Por su parte, el receptor es responsable de garantizar que los datos portados sean pertinentes y no excesivos para el nuevo tratamiento; por ello, en caso los datos personales transferidos no sean pertinentes o resulten excesivos, no deberán guardarse ni tratarse. Para evitar o mitigar dicha situación, es necesario establecer de forma clara y

cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

directa el propósito del nuevo tratamiento antes de cualquier solicitud de transmisión. Así, todo responsable debe estar preparado para facilitar el ejercicio de este derecho.

- La portabilidad de los datos frente a otros derechos de los titulares de los datos personales: este se ejerce sin perjuicio de otros derechos. Podrá seguir usándose el servicio del responsable del tratamiento y beneficiándose de él, incluso, después de una operación de portabilidad de datos en tanto el responsable siga tratándolos. El Grupo de Trabajo 29 (2017) enfatiza que, en caso existan leyes sectoriales europeas o de Estados Miembros que regulen la portabilidad de datos y resulten aplicables, deberán también ser tomadas en cuenta a la hora de responder a una solicitud de portabilidad, en virtud del RGPD; es necesario evaluar, caso por caso, de qué manera dicha legislación concreta puede afectar al derecho a la portabilidad.

A nivel regional, resaltan los siguientes referentes legislativos:

- La propuesta legislativa acordada, con carácter orientativo, en los Estándares de protección de datos para los países Iberoamericanos aprobados por la Red Iberoamericana de Protección de Datos [RIPD] (2017), de la cual el Perú es país miembro:

  > 30.1. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.
  > 30.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.
  > 30.3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

> 30.4. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieran sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

- En los Estados Unidos Mexicanos, el artículo 57° de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [LGPDPPSO] (2017) dispone lo siguiente:

> Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales. El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

- En Argentina, el artículo 33° del Proyecto de Ley N° 2986/20, Proyecto de Ley sobre Protección de Datos Personales [Proyecto de Ley N° 2986/20] señala lo siguiente:

> Si se brindan servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización. El titular de los datos puede solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.
>
> Este derecho no procederá cuando:
>
> a) Su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el responsable o encargado del tratamiento.
>
> b) Vulnere la privacidad de otro titular de los datos.
>
> c) Vulnere las obligaciones legales del responsable o encargado del tratamiento.
>
> d) Impida que el responsable del tratamiento proteja sus derechos, su seguridad o sus bienes, o los derechos, seguridad y bienes del encargado del tratamiento, o del titular de los datos o de un tercero.

- En Ecuador, recientemente, el 26 de mayo de 2021, se publicó en el Registro Oficial Suplemento N° 459, Ley Orgánica de Protección de Datos Personales [LOPDP], que, en su artículo 17°, sostiene lo siguiente:

> El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables. La Autoridad de Protección de Datos Personales deberá dictar la normativa para el ejercicio del derecho a la portabilidad.
>
> El titular podrá solicitar que el responsable del tratamiento realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de

datos por parte del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación. El responsable que ha recibido la información asumirá las responsabilidades contempladas en esta Ley. Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones:

1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular.

2) Que el tratamiento se efectúe por medios automatizados.

3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente ley.

4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita y sin trabas.

No procederá este derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido

sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

3.2.1 Tipo de tratamiento y fuentes de recopilación aplicables

A continuación, se analizará qué condiciones y/o supuestos son comunes para la aplicación del derecho a la portabilidad. La RIPD (2017) incidió en que el derecho a la portabilidad aplique a aquellos datos personales que sean objeto de tratamiento, ya sea por vía electrónica o medios automatizados[214], y sin ninguna limitación a la fuente por la que se hayan obtenido los datos personales.

No obstante, el Proyecto de Ley (2021) sigue, en gran medida, la recomendación de la RIPD (2017), aunque incorpora ciertos límites adicionales a su aplicación, ya que solo será ejercible cuando "a) el tratamiento esté basado en el consentimiento o en una relación contractual en la que el titular del dato es parte" y, adicionalmente, "b) el tratamiento se ejerza mediante medios automatizados". Es de notar que su redacción guarda más similitud con el RGPDP (2016), que procede si el tratamiento está basado en el consentimiento o en un contrato; y, el tratamiento se efectúa por medios automatizados, es decir, ambos incluyen las mismas limitaciones a la fuente de obtención de los datos personales[215]. Tampoco incluyen junto a la vía automatizada la alusión a la vía electrónica. Además, indican que solamente podrá ejercerse la transferencia directa entre responsables del tratamiento en tanto sea técnicamente posible.

---

[214] Podría decirse que medios automatizados sería un término más amplio que lo electrónico, pues segúnla DRAE (s.f.) la automatización implica "aplicar la automática a un proceso o a un dispositivo", siendo esta la "ciencia que trata de sustituir en un proceso el operador humano por dispositivos mecánicos o electrónicos". Sin embargo, resulta conveniente que ambas acepciones sean usadas intercambiablemente e interpretadas lo más ampliamente posibles, sobre todo, en el sector digital donde se busca que la portabilidad pueda ejercitarse en línea.

[215] El RGPDP (2016) es aún más incisivo pues, pese a haber indicado que solo aplica cuando media consentimiento o un contrato, en el siguiente numeral 3 de su artículo 20º indica que "tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público".

En la LGPDPPSO (2017) mexicana, se comprende aquellos datos personales que se conserven en un sistema de tratamiento automatizado, pero dividido en dos (2) supuestos, algo distinto a lo recomendado por la RIPD (2017):

(i) El titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. En este primer supuesto, al igual que la RIPD (2017), en contraste con el Proyecto de Ley (2021), no se indica que deberá mediar consentimiento o una relación contractual de la que el titular del dato sea parte.

(ii) Solo se tendrá derecho a transmitir dichos datos personales de un responsable a otro y sin impedimentos del responsable del tratamiento, si es que el tratamiento se basa en el consentimiento o en un contrato. Si bien recoge limitaciones similares al Proyecto de Ley (2021), no se indica que será procedente cuando sea técnicamente posible, ya que será ejercible sin impedimentos del responsable del tratamiento.

Para Argentina, el Proyecto de Ley N° 2986/20 indica que será aplicable en caso se brinden "servicios en forma electrónica que incluyan el tratamiento de datos personales". El titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento, en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización. Seguidamente, se podrá solicitar su transferencia directa, de responsable a responsable, cuando sea técnicamente posible.

Finalmente, en la legislación ecuatoriana (2021), el responsable del tratamiento deberá transferir o realizar la comunicación de los datos personales a otro responsable "en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de los datos". A diferencia de los anteriores, es necesario que se produzca, al menos, una de las siguientes condiciones para su ejercicio: se haya otorgado consentimiento para el tratamiento para uno o varios

fines específicos, cuando la operación sea técnicamente posible, sino serán transmitidos directamente al titular; se efectúe el tratamiento por medios automatizados; se trate de un volumen relevante de datos personales, según los parámetros de su reglamentación; o, sea necesario el tratamiento para el cumplimiento de obligaciones y el ejercicio de derechos del encargado o titular, en el ámbito del derecho laboral y seguridad social.

Por ello, la postura más adecuada resulta ser la propuesta por el RIPD (2017). No resulta adecuado ni deseable establecer mayores límites al ejercicio del derecho a la portabilidad de datos, como lo sería el segregar los datos, pese a ser automatizados y por ende ser técnicamente susceptibles de portar, por las fuentes de obtención al establecer mayores límites como que solo será ejercible cuando "a) el tratamiento esté basado en el consentimiento o en una relación contractual en la que el titular del dato es parte" y, adicionalmente, "b) el tratamiento se ejerza mediante medios automatizados". Por eso, aquellos datos personales que no hayan sido obtenidos concurrentemente en el marco de ambos supuestos, quedarían exceptuados de su ejercicio. Lo anterior, por supuesto, supone establecer límites innecesarios y debilitar el control del titular de los datos personales injustificadamente.

3.2.2 Sujetos aplicables

El RGPDP (2016) es explícito al indicar, en el artículo 20.3º, que tal derecho "no aplica en el ejercicio de poderes públicos conferidos al responsable del tratamiento". Sin embargo, el RIPD (2017) no hace distinción o limita a qué tipos de responsables del tratamiento le serán aplicables. Por ello, se aplica a responsables del tratamiento del sector público y privado.

Para el caso peruano, el propuesto artículo 23-Aº del Proyecto de Ley (2021) sí precisa que el derecho a la portabilidad de datos aplicaría solo a responsables del tratamiento en el sector privado. Ello en tanto se indica que "nose aplica para el cumplimiento de las competencias o funciones conferidas a las entidades públicas".

En México, la LGPDPPSO (2017) aplica solo "en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos". Por ello, la portabilidad de datos personales solo puede ejercerse en el ámbito público. Así, es de mencionar que, para el caso de datos personales en el sector privado, resulta aplicable la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que data del año 2010, y resulta aplicable a "los particulares, sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales". No obstante, dicha normativa no contempla el derecho a la portabilidad de datos personales.

Para Argentina, el Proyecto de Ley N° 2986/20 abarca a ambos sectores. El artículo 33° no hace mayor distinción frente a qué responsables puede ser ejercido el derecho a la portabilidad, es decir, si aquellos comprendidos en el sector público y/o privado o bajo. Al no distinguirse, se precisa que, bajo dicha legislación, el responsable de tratamiento es en principio toda "persona humana o jurídica, pública, privada o mixta".

En Ecuador, la LOPDP (2021) es aplicable a toda "persona natural o jurídica, pública o privada, autoridad pública, u otro organismo".

Como se observa, en algunos países se ha previsto que el derecho a la portabilidad de datos personales sea aplicable también al sector público e, incluso, a ambos sectores público y privado. Resultaría deseable que para extender los efectos de este derecho este sea aplicado a ambos sectores. No obstante, como se ha mencionado en las secciones anteriores, también se vienen desarrollando múltiples iniciativas, sobre todo, a cargo de la SGTD para promover la transformación digital, siendo uno de sus objetivos implementar la interoperabilidad y portabilidad de datos entre entidades públicas, incluyendo a privados. En ese sentido, el derecho a la portabilidad de datos podría incluso fortalecer y complementar dichas estrategias de transformación digital. No se observa motivación suficiente de porqué, salvando las excepciones justificadas y/o legales-, limitar la aplicación de este derecho frente al sector público. Sin

embargo, el enfoque de esta investigación se centró en el sector privado, por lo que en esta ocasión es prioritario proponer la regulación de portabilidad de datos personales del sector privado. Además, es en este sector donde más urgen estas iniciativas, pues como se mencionó el sector público viene atravesando un amplio sistema de transformación digital.

3.2.3 Excepciones a su ejercicio y/o causales de improcedencia

El artículo 30.3º de la RIPD (2017) indica que el derecho a la portabilidad "no afectará negativamente a los derechos y libertades de otros". Una segunda limitación está contenida en el artículo 32.2º que dispone que los Estados Iberoamericanos deberán incorporar las causales de improcedencia al ejercicio de los derechos ARCO[216] y de portabilidad que, de manera limitativa mas no enunciativa, podrán ser: cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público; el tratamiento sea necesario para el ejercicio de las funciones propias de autoridades públicas; el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular; el tratamiento sea necesario para el cumplimiento de una disposición legal; y, los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

El Proyecto de Ley (2021) no determina algún supuesto de excepción o improcedencia más allá de que no fuese técnicamente posible la transferencia. No obstante, debe considerar que, de manera genérica, en la vigente LPDP (2011), el artículo 27° dispone que, con respecto a los titulares y encargados de tratamiento de administración pública, podrán denegar el ejercicio de los derechos de acceso, supresión y oposición por razones fundadas en la protección de derechos e intereses de terceros, cuando ello pueda obstaculizar actuaciones judiciales o administrativas en curso o si así lo dispusiera la ley.

Si bien indica expresamente a titulares y encargados de administración pública, también se extiende a los comprendidos en el sector privado, pues, en el ejercicio de los derechos, existe la posibilidad de que el responsable o encargado

[216] Los derechos ARCO significa acceso, rectificación, cancelación y oposición.

deniegue su ejercicio por razones motivadas en la ley (lo que comprende no vulnerar derechos de terceros). Prueba de ello es que el artículo 59° del Reglamento (2013) dispone, sin distinguir entre públicos y privados, que la respuesta total o parcialmente negativa, ante la solicitud de un derecho del titular de datos personales, debe estar debidamente justificada y precisa señalar el derecho que le asiste al mismo a reclamar ante la Dirección General de Protección de Datos Personales.

En el RGPDP (2016), se prevé que, cuando sea técnicamente posible, podrán transferirse los datos personales de un responsable a otro. Posteriormente, se precisa que tampoco aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, ni afectará negativamente a los derechos y libertades de otros.

Para México, tampoco se prevén mayores limitaciones. Por el contrario, la LGPDPPSO (2017) indica que, en el caso de la transferencia entre responsables, esta debe realizarse "sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales".

El Proyecto de Ley N° 2986/20, en Argentina, señala que la transferencia entre responsables se hará cuando sea técnicamente posible. Adicionalmente, tal derecho no procederá en cuatro (4) supuestos, si su ejercicio impone una carga financiera o técnica excesiva o irrazonable al responsable o encargado del tratamiento; si vulnera la privacidad de otro titular de los datos; si vulnera las obligaciones legales del responsable o encargado del tratamiento; o, si impide que el responsable del tratamiento proteja sus derechos, seguridad y bienes, el del encargado del tratamiento, titular de los datos o un tercero.

Ecuador, la LOPDP (2021) también contempla que solo "en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento", se podrá transmitir de un responsable a otro directamente los datos personales. Asimismo,

si bien no se mencionan mayores limitaciones, es porque dicho derecho solo procederá en tanto se produzca, al menos, una (1) de las cuatro (4) condiciones que ya fueron enlistadas en la sección anterior.

Así, los motivos de improcedencia más razonables que deberían ser recogidos son cuando (i) no fuese técnicamente posible la transferencia, lo que incluye que su ejercicio imponga una carga financiera, técnica excesiva o irrazonable al responsable o encargado del tratamiento; (ii) se vulnere la protección de derechos de terceros (incluidos otros titulares de datos personales también); (iii) con ello, se pueda obstaculizar actuaciones judiciales o administrativas en curso; y, (iv) otras excepciones legales.

3.2.4 Tipos de datos aplicables

El RGPDP (2021) fue la primera legislación en indicar que los datos personales aplicables serían aquellos que le incumban y que haya facilitado a un responsable del tratamiento; además, precisa que no afectará negativamente derechos ni libertades de otros (terceros). A lo que el Grupo de Trabajo 29 (2017) ha indicado que ello genera solo aplique a los siguientes datos personales:

- Que incumban al interesado implica que quedan excluidos los datos anónimos o que no conciernan al titular de los datos personales, pero se incluyen datos seudónimos claramente vinculados con el titular (un ejemplo, al mediar un identificador para el sujeto). Sobre la información que contenga datos de terceros (registros telefónicos, mensajería interpersonal o de transmisión de voz por internet con detalles de terceros participantes en llamadas), no deberá hacerse una interpretación excesivamente restrictiva, debiendo permitirse portar los datos que tambiénincumben a su titular, pero dicho nuevo responsable no deberá tratarlos para fines que afecten negativamente derechos y libertades de terceros.

- Facilitados por el interesado: ello comprende a los datos facilitados de forma activa y consciente por el interesado (por ejemplo, dirección postal, nombre de usuario, edad, etc.); datos observados facilitados por el

interesado en virtud del uso de un servicio o dispositivo (por ejemplo, historial de búsqueda, datos de tráfico y de ubicación) y otros datos en bruto tales como el ritmo cardiaco registrado por un dispositivo ponible. No comprende los datos inferidos y deducidos que son creados por el responsable del tratamiento sobre la base de los datos facilitados por el interesado, es decir, que se infieran o se deduzcan del análisis de los datos facilitados (por ejemplo, datos generados con motivo del perfilamiento o resultados algorítmicos y puntuaciones).

- No afectará negativamente a los derechos y libertades de otros: primero, ello implica que, con respecto a los datos personales de terceros, a fin de evitar dichos efectos negativos, el tratamiento por el responsable del tratamiento receptor se permite solo en la medida en que los datos se mantengan bajo el control exclusivo del usuario solicitante y se gestionen solo para necesidades puramente personales o domesticas; no podrá utilizar los datos de terceros que se le transmitan para sus propios fines; la aplicación de herramientas que permitan a los interesados seleccionar los datos relevantes que desean recibir, transmitir y excluir de otras personas es una buena práctica para todos los responsables del tratamiento (remitentes y receptores); igualmente, para otros interesados involucrados que estén dispuestos a dar su consentimiento, podría ser una buena práctica a seguir.

  Segundo, sobre los datos protegidos por la propiedad intelectual y los secretos comerciales, estos derechos deben tomarse en consideración antes de responder a una solicitud de portabilidad de datos, pero no deben generar la negativa a proporcionar toda la información al interesado. Un posible riesgo empresarial, en sí mismo, no es base para negarse a responder a la solicitud de portabilidad, los responsables del tratamiento podrán transmitir los datos personales facilitados por los interesados sin revelar información protegida por secreto comercial o derechos de propiedad intelectual.

Por su parte, el Proyecto de Ley (2021) solo indica que el titular tiene derecho a recibir los datos personales “sobre sí mismo, que haya facilitado”. Sin

embargo, ello no delimita si se refiere a datos facilitados de forma activa y consciente por el interesado (por ejemplo, dirección postal, nombre de usuario, edad, etc.) y/o a datos observados facilitados por el interesado en virtud del uso de un servicio o dispositivo.

Tampoco brinda mayores luces si aplicaría datos personales de terceros, por ejemplo, una fotografía de varias personas, un post en una red social o en un foro, un correo electrónico o documento con intervención de al menos dos personas naturales; e, información que, pese a contener datos personales, se encuentra exceptuada del derecho a la portabilidad de datos por implicar información confidencial u otros derechos de terceros como los de propiedad intelectual o el secreto empresarial, como es el caso de los datos derivados o inferidos, que son producto del análisis realizado a los datos personales que fueron otorgados por el titular de los datos personales. De igual manera, si aquellos datos anonimizados y disociados estarán sujetos al ejercicio del presente derecho.

Como referencia al posible reconocimiento de estos límites en la LPDP (2011), el contenido del derecho de acceso establece que este no podrá revelar datos pertenecientes a terceros, aun cuando los mismos se vinculen con el interesado. Así, la autoridad, en la Resolución Directoral Nº RD-044-2015-DGPDP, ha señalado que la solicitud de acceso debe corresponder exclusivamente a los datos personales del titular y no a terceros; por ello, tampoco implica obtener información de los bancos de datos personales, lo cual significa que no comprenderá el acceso a documentos ni otros datos concretos que puedan contener información protegida de terceros, es decir, documentos de seguridad de la información, información confidencial, secreto empresarial, datos que califican como información confidencial o están protegidos por derechos de propiedad industrial o incluso por secreto empresarial.

Sin embargo, dichos límites, pese a ser totalmente aplicables al ejercicio de tal derecho, no han sido considerados o adecuadamente regulados en el Proyecto de Ley (2021), como sí ocurre en el RGPDP (2016) gracias a la labor del Grupo de Trabajo 29 (2017).

En esta línea, debe advertirse que cuando se ha realizado un procedimiento de disociación o anonimización sobre los datos personales, la LPDP (2011) y su Reglamento (2013) reconocen que ya no serán aplicables múltiples obligaciones legales, como obtener el consentimiento previo (artículo 14.8º de la LPDP, 2011); medidas de seguridad para el flujo transfronterizo (artículo 15.6º de la LPDP, 2011); demás obligaciones sobre supresión de los datos personales y utilización de datos personales para finalidades distintas a las consentidas por el titular de los datos personales (artículos 28.4º y 28.7º, de la LPDP, 2011); protección en caso de denegación de ejercicio de derechos de supresión o cancelación (artículo 70º del Reglamento, 2013); y, como excepción a la comisión de varias infracciones (artículo 132º del Reglamento, 2013).

Para el caso de México, la LGPDPPSO (2017) también alude a aquellos datos que el titular de los mismos haya facilitado y, posteriormente, se repite cualquier otra información que haya facilitado. Por ello, se puede decir que debe entenderse de forma amplia, incluyendo aquellos datos facilitados de forma no directa u observados.

En la legislación argentina, el Proyecto de Ley N° 2986/20 indica que se tiene derecho a "obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento". Si bien no contiene expresamente a qué tipos de datos personales aplicarían, puede que algunas limitaciones le resulten aplicables. Estas serían no vulnerar (i) la privacidad de otro titular; (ii) las obligaciones legales del responsable o encargado del tratamiento; e, (iii) impedir que el responsable del tratamiento proteja sus derechos, seguridad y bienes, o los del encargado del tratamiento, titular de los datos o de un tercero. Por ello, tales disposiciones legales sugieren que, probablemente, el ejercicio del derecho a la portabilidad no sea aplicable a los datos personales de otros titulares y datos de terceros sujetos a derechos de propiedad intelectual, secreto comercial u otras obligaciones. En ese sentido, puede que se argumente que, por tales disposiciones, los datos inferidos y derivados, así como los datos anonimizados y disociados tampoco estarían comprendidos en el ejercicio de dicho derecho al no ser compatibles con algunas de las tres (3) limitaciones anteriores.

En el marco ecuatoriano, siguiendo cabalmente la recomendación del RIPD (2017), la LOPDP (2021) indica idénticamente a la fórmula recomendada, donde el titular puede solicitar la portabilidad o comunicación sobre sus datos, detallando que no procede cuando se trate de lo siguiente:

> [I]nformación inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

Sin embargo, no hace mayor alusión a los datos personales ni privacidad de otros titulares de datos personales, mientras que la RIPD (2017) sí deslinda que "no afectará negativamente derechos ni libertades de otros". Finalmente, sobre los datos anonimizados y disociados, puede deducirse que, en base a dicha proscripción citada, tampoco se encuentran comprendidos dentro del ejercicio del derecho en cuestión.

Con todo, los tipos de datos personales aplicables deberían ser los siguientes:

- Todos aquellos datos personales otorgados directa e indirectamente por su titular, es decir, incluir a los datos observados y a los datos en bruto generados en la recolección.

- Los derivados e inferidos como una buena práctica comercial siempre que no se genere ninguna vulneración de terceros, es decir, que se respeten los derechos de propiedad intelectual y secreto comercial. Lo anterior, teniendo en cuenta que un posible riesgo empresarial en sí mismo no deberían considerarse una negativa justificada para no incluir tales datos personales en la solicitud de portabilidad.

- Los datos anonimizados no deberían incluirse, pero sí los personales que fueron disociados, en tanto se encuentren claramente vinculados con su titular.

- Los datos personales con o sobre otros terceros, no debiendo hacerse una interpretación excesivamente restrictiva a efectos de permitirse portar los datos que también incumban a su titular, pero tomando en cuenta que el nuevo responsable no deberá tratarlos para fines que afecten negativamente derechos y libertades de terceros. Además, resultaría deseable promover la implementación de herramientas que permitan recabar el consentimiento informado, libre, previo expreso e inequívoco de aquellos otros titulares de los datos personales en caso desearan permitir que sus datos personales involucrados sean portados por el solicitante de la portabilidad de sus datos personales.

3.2.5 Tipos de soportes y formatos aplicables

El RIPD (2017) sostiene que el titular de los datos personales tendrá derecho a obtener una *copia* de los datos personales, "en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera", cuando sea técnicamente posible.

El RGPDP (2016) dispone que debe emplearse un formato que permita su reutilización. Para ello, deberá usarse "un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado (…) directamente de responsable a responsable cuando sea técnicamente posible. En el considerando 68º del RGPDP (2016), se "alienta a los responsables del tratamiento a crear formatos interoperables que permitan la portabilidad de los datos, pero sin obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles".

Así, el Grupo de Trabajo 29 (2017) indica que los términos "estructurado, de uso común y de lectura mecánica constituyen un conjunto de requisitos mínimos que deben facilitar la interoperabilidad del formato de los datos proporcionado (…) son especificaciones relativas a los medios, mientras que la interoperabilidad es el resultado deseado" (p.19). Pero, ¿qué significan tales requisitos?

- Lectura mecánica y de uso común: según lo indicado por el Grupo de Trabajo del Consejo de la Unión Europea, en el glosario del Identificador Europeo de Legislación [ELI] (2019), significa que los datos deben estar en un formato que una computadora pueda leer y procesar automáticamente, como es el caso de estos datos comúnmente utilizados CSV, JSON, XML, etc. Además, los datos legibles por máquina deben ser datos estructurados.

- Estructurado: según el glosario de la Open Knowlegde Foundation (s.f.), se refiere a datos en los que la relación estructural entre elementos es explícita en la forma en que los datos se almacenan en un disco de computadora. XML y JSON son formatos comunes que permiten representar muchos tipos de estructura. Esto no sucede con documentos de Word o PDF que, si bien reflejan la posición de las entidades en la página, resulta difícil extraer su estructura interna de forma automática.

El Grupo de Trabajo 29 (2017) propone que los datos personales "se proporcionen en formatos que tengan un elevado nivel de abstracción", cuando no existan formatos de uso común en un sector o contexto determinados. Los responsables del tratamiento deben proporcionar los datos personales, utilizando formatos abiertos de uso común como XML, JSON, CSV, pero dando los metadatos[217] útiles que precisen el significado de la información intercambiada y permitan la reutilización de los datos con el mejor nivel posible de abstracción sin revelar derechos de terceros. Por ejemplo, se indica que brindar versiones en PDF

[217] No obstante, procesar metadatos adicionales con el único fin de que puedan necesitarse o requerirsepara responder a una solicitud de portabilidad de datos no supone una justificación legítima para dicho tratamiento.

de una bandeja de entrada de correos electrónicos incumple el nivel de estructurabilidad y descripción requeridos para la reutilización. Por ello, resulta interesante que un responsable del tratamiento ofrezca al interesado opciones a elegir el formato preferido para los datos personales, pero junto con ello debería también ofrecer una explicación clara de la repercusión de dichas opciones.

Como se observa, no existen recomendaciones o disposiciones específicas sobre qué formatos proporcionar, pues hay innumerables posibles tipos de datos que podrían ser tratados por un responsable del tratamiento. Se considera que el formato más apropiado diferirá entre los diversos sectores y "puede que ya existan formatos adecuados que siempre deberían elegirse con el fin de lograr el propósito de que sean interpretables y permitan al interesado un alto grado de portabilidad de los datos" (Grupo de Trabajo, 2017, p.20). Sin embargo, tal Grupo de Trabajo (2017) sí indica que "los formatos que estén sujetos a costosas limitaciones de licencia no deben considerarse una opción adecuada" (p.20). Además, alienta a la "cooperación entre las partes interesadas del sector y a las asociaciones comerciales para que trabajen conjuntamente sobre un conjunto de normas y formatos interoperables comunes que respondan a los requisitos del derecho a la portabilidad de los datos" (Grupo de Trabajo, 2017, p. 20).

En sede nacional, el Proyecto de Ley (2021) también señala que será un formato estructurado, de uso común y lectura mecánica, pudiendo transmitirse directamente "cuando sea técnicamente posible". No obstante, no se ha realizado mayor desarrollo sobre los formatos deseados u otras especificaciones técnicas deseables para su implementación.

En el marco mexicano, la LGPDPPSO (2017) sostiene que el titular podrá recibir copia de los datos objeto de tratamiento, en un "formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos", así como a transmitirlos "conservados en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales". Finalmente, se indica que será el Sistema Nacional, el cual, vía lineamientos,

emita “los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales” (LGPDPPSO, 2017).

De igual manera, el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018) indica, en elartículo 6° de los “Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales”, que existen los siguientes criterios para considerar a un formato como estructurado ycomúnmente utilizado:

> [S]e entenderá que un formato adquiere la calidad de estructurado y comúnmente utilizado, con independencia del sistema informático utilizado para su generación y reproducción, cuando se cumplan todos los siguientes supuestos:
> I. Se trate de un formato electrónico accesible y legible por medios automatizados, de tal forma que éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos.
> II. El formato permita la reutilización y/o aprovechamiento de los datos personales.
> III. El formato sea interoperable con otros sistemas informáticos, de conformidad con lo dispuesto en el artículo 2º, fracción I de los presentes Lineamientos [Interoperabilidad: capacidad de los responsables transmisor y receptor para compartir infraestructura y datos personales a través de la conexión de sus respectivos sistemas o plataformas tecnológicas].

Para el Proyecto de Ley N° 2896/20 argentino, se ha previsto que el titular de los datos tiene derecho a obtener copia de los datos personales objeto de tratamiento “en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización”. Asimismo, podrá “solicitar que sus datos personales se

transfieran directamente de responsable a responsable cuando sea técnicamente posible".

En Ecuador, la LOPDP (2021) prescribe que el titular de los datos personales podrá recibir copia de sus datos facilitados en "un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características". Asimismo, se podrá solicitar la transferencia o comunicación a otro responsable del tratamiento "en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento" (LOPDP, 2021). Finalmente, señala que es la Autoridad de Protección de Datos Personales quien deberá dictar la normativa para el ejercicio del derecho a la portabilidad.

3.3 Particularidades adicionales para la portabilidad de datos personales

A continuación, se señalan algunos aspectos adicionales que se deben considerar en la regulación a la portabilidad de datos personales nacional, ya sea en vía legislativa o regulatoria, a efectos de garantizar su adecuado ejercicio y promoción en el sector privado.

3.3.1 Gratuidad en la atención de la solicitud de portabilidad

El artículo 53° del Reglamento (2013) sostiene que debe establecerse un procedimiento sencillo para el ejercicio de los derechos reconocidos por esta normativa. Además, existe libertad y/o flexibilidad en los mecanismos a implementarse para el ejercicio de los derechos del titular, siempre que sea para su beneficio.

El ejercicio de los derechos ante los bancos de datos personales de administración privada es de carácter gratuito, salvo lo establecido en normas especiales de la materia. Dicho artículo indica que "no se podrá establecer como medios para el ejercicio de los derechos ninguno que implique el cobro de una tarifa adicional al solicitante o cualquier otro medio que suponga un costo

excesivo". Por ello, cabe la duda si el eventual cobro de una tarifa proporcional sería posible y bajo qué motivos.

Al respecto, cabe traer a colación el análisis del Grupo de Trabajo 29 (2017) que realiza sobre el RGPDP (2016). En principio, el artículo 12° del RGPDP (2016), al igual que el artículo 53° del Reglamento (2013), prohíbe al responsable del tratamiento cobrar un canon por facilitar los datos personales, a menos que pueda demostrar que las solicitudes son manifiestamente infundadas o excesivas -especialmente por su carácter repetitivo[218]-. Ahora, la aplicación de sistemas automatizados, como las API, pueden facilitar los intercambios con el interesado, reduciendo así la carga que producirían repetitivas solicitudes a los responsables del tratamiento; ello minimiza las situaciones de negativas justificadas a no entregar la información solicitada, incluso ante múltiples solicitudes de portabilidad de datos de un mismo titular de datos personales.

Además, se advierte que el costo total de implementar canales, procesos o vías para la atención de dicho nuevo derecho y el número total de solicitudes que puedan ser recibidas, no podrán ser utilizados como justificación para una negativa a la solicitud de su ejercicio. Es decir, no podrá aducirse que la atención a dicha solicitud de portabilidad de datos personales resulta excesiva. Por el contrario, podrán cobrarse o trasladarse dichos dos (2) costos señalados en la oración anterior a los titulares de los datos personales.

Dicho análisis resulta acertado, ya que, de lo contrario, se desnaturalizaría el carácter gratuito del ejercicio de los derechos del titular de los datos personales.

[218] El artículo 12.5º prohíbe al responsable del tratamiento cobrar un canon por facilitar los datos personales, a menos que dicho responsable pueda demostrar que las solicitudes son manifiestamenteinfundadas, excesivas y/o de carácter repetitivo:

> Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

Ni los costos de implementación de los canales, procesos o vías para la atención del derecho a la portabilidad de datos personales, ni otras solicitudes previas deberían ser cobrados al titular.

El eventual cobro de un canon o tarifa adicional deberá ser justificado si implica la asunción de un costo adicional. Esto podría suceder en el caso análogo del derecho de acceso, del material impreso de la información y ulterior envío a un punto de destino a petición del titular de los datos personales; ello siempre que se informe previamente del costo total y conceptos. Inclusive, siempre debería procurarse no cobrar costo alguno. No obstante, en el caso del derecho a la portabilidad, como señala el Grupo de Trabajo 29 (2016), el tratamiento automatizado y más el uso de herramientas, como las API o, incluso, la descarga de información directa por el propio usuario (ambas modalidades convencionales para cumplir con la solicitud de portabilidad), difícilmente, suponen un costo específico adicional alguno en recursos humanos y/o técnicos, destinados a la atención de una solicitud de portabilidad de datos personales.

Ello reduce el espectro de posibilidades tanto de cobro de una tarifa adicional como de negativa justificada por exceso o reiteración de solicitudes del ejercicio del derecho en cuestión. En todo caso, el responsable del tratamiento tiene en su poder la disposición de elegir las vías más adecuadas para el cumplimiento de dicho deber, siempre en beneficio del titular de los datos personales. Debe considerar, hasta cierta medida, la posibilidad del ejercicio reiterativo y masivo de dicho derecho, más aún conforme al alcance del tratamiento y demás actividades que realice en el mercado.

3.3.2 Requisitos de la solicitud y validación del consentimiento

El artículo 50º del Reglamento (2013) indica que toda solicitud de ejercicio de los derechos deberá contener lo siguiente: nombres y apellidos del titular del derecho y acreditación de los mismos, y en su caso de su representante; petición concreta; domicilio, o dirección que puede ser electrónica, a efectos de las notificaciones que correspondan; fecha y firma del solicitante, pudiendo ser

pudiendo ser también electrónica y/o digital, según la normativa vigente; y, documentos que sustenten la petición, de ser el caso.

Cabe resaltar que, con respecto a la necesidad de autenticación, el RGPDP (2016) difiere a la LPDP (2011), pues si bien existe la necesidad de autenticar al titular de los datos personales para determinar con certeza la identidad del titular de los datos personales, reconoce que en muchos casos estos procedimientos ya existen: "los datos personales utilizados para registrar a la persona a la que concierne el tratamiento pueden utilizarse también como prueba para autenticar con fines de portabilidad" (Grupo de Trabajo 29, 2017, p. 16); por ejemplo, los nombres de usuarios y contraseñas se utilizan con frecuencia para permitir a las personas acceder a sus datos en las cuentas de distintos servicios digitales "algunos de los cuales se usan sin que el individuo revele su nombre completo e identidad" (Grupo de Trabajo 29, 2017, p. 16).

Por su parte, la LPDP (2011) dispone que para el ejercicio debe proporcionarse "nombres y apellidos del titular del derecho y acreditando los mismos", sin abrir la posibilidad a otros mecanismos de autenticación más acorde al tratamiento automatizado en los servicios digitales.

Asimismo, para el caso del ejercicio del derecho a la portabilidad de los datos, si bien existe el requisito de emitir la petición concreta en la solicitud, resulta necesario que, al momento de emitirse, se detalle si se desea obtener una copia de los datos personales para sí mismo y/o transmitirlos directamente a otro responsable del tratamiento. Para lo segundo, resulta deseable el dar suficientes detalles de la identidad del receptor a efectos de validar que ese el destinario indicado. Para ello, al menos, deberían detallarse los siguientes datos de contacto: si es a otra persona natural, su nombre completo, DNI u otro documento de identidad y alguna vía de contacto adecuada para entablar la comunicación y transmisión de los datos (por ejemplo, correo electrónico, cuenta de alguna red social, o hasta dirección física); y, si es a una persona jurídica, la razón/denominación social y N° RUC o código de identificación tributaria, cuando no pueda ponerse en contacto directamente.

Sin embargo, es de notar que, en algunos casos de transferencia a terceros proveedores de servicios digitales, no resultará necesario brindar detalles como la razón social o un código de identificación tributaria, sino que otros mecanismos más sencillos o directos, como el url del sitio web o de la cuenta del titular de los datos personales en dicho servicio digital (red social, correo electrónico, etc.), sería suficiente para saber con certeza a quién y donde transferir.

3.3.3 Consideraciones adicionales del Grupo de Trabajo 29

El Grupo de Trabajo 29 (2017) indica que deben considerarse comoimpedimentos del responsable del tratamiento para transmitir directamente los datos personales a cualquier obstáculo legal, técnico o financiero. Ello en tanto los mismos sean impuestos por el responsable del tratamiento para evitar o ralentizar el acceso, la transmisión o la reutilización de sus datos personales vía el propio interesado o por parte de cualquier otro responsable del tratamiento designado. Ejemplos de dichos obstáculos serían (i) los cánones exigidos para laentrega de los datos; (ii) la falta de interoperabilidad o acceso a un formato de datos o a una API o el formato proporcionado; (iii) la excesiva dilación ocomplejidad para recuperar un conjunto completo de datos; (iv) el enmascaramiento deliberado de un conjunto de datos; y, (v) la normalización sectorial o exigencias de acreditación específicas, injustificadas o excesivas.

Es cierto que también indica que la trasmisión directa de un responsable del tratamiento a otro puede tener lugar si es posible la comunicación entre dos sistemas, pero de manera segura. Por eso, se entiende a través de una comunicación autenticada con el nivel necesario de cifrado de los datos y "cuando el sistema receptor cuente con las condiciones técnicas necesarias para recibir los datos entrantes" (Grupo de Trabajo, 2017, p.18). Dicho grupo reconoce que, de existir dificultades técnicas que impiden la transmisión directa, se "explicará a los interesados cuáles son dichas dificultades y su decisión tendrá un efecto similar a la negativa a dar curso a una solicitud del interesado" (Grupo de Trabajo, 2017, p. 18), es decir, es una negativa justificada.

Sin embargo, dicho Grupo de Trabajo (2017) precisa que técnicamente deben valorarse dos vías distintas y complementarias para ejercer la portabilidad: (i) vía transmisión directa del conjunto completo de datos que se pueden portar o varios extractos de partes de dicho conjunto y (ii) vía una herramienta automatizada que permita la extracción de los datos pertinentes. La segunda vía será más útil para conjuntos de datos de gran volumen y complejidad. Esto permite la extracción de cualquier parte del conjunto de datos que resulte pertinente para el interesado en el contexto de su solicitud, lo que contribuye a minimizar los riesgos y, posiblemente, permita el uso de mecanismos de sincronización de datos deseables para comunicaciones periódicas entre responsables del tratamiento, permitiendo actualizar los datos personales.

Finalmente, en la Unión Europea, se proponen distintos ejemplos o herramientas para cumplir con dichas dos vías: la mensajería segura, un servidor SFTP[219] o una API[220]. También, precisa que debe permitírsele a los titulares de los datos personales usar depósitos de datos personales, las PIMS (ya desarrolladas en el capítulo anterior) u otros servicios proveídos por terceros de confianza para conservar, acceder y tratar sus datos personales, conforme a lo que se establezca o solicite al responsable del tratamiento.

Para ello, y como parte del deber de información que será abordado más abajo, es crucial que en sede nacional se disponga que el titular de los datos

[219] Es la abreviatura al SSH File Transfer Protocol [Protocolo de Transferencia de Archivos SSH] o Secure File Transfer Protocol [Protocolo de Transferencia de Archivos Seguro]. Este protocolo de transferencia de archivos por omisión es preferido en tanto que, a diferencia de otros, como el tradicional File Transfer Protocol [FTP], realiza transferencias mediante un canal único Secure Shell [SSH], que es un protocolo criptográfico que ofrece acceso seguro al servidor en la red y permite autenticar al cliente, utilizando un usuario, contraseña y claves criptográficas. Por su parte, el FTP utiliza dos canales separados para transferir información sin encriptar, generando riesgos ante ataques o intromisiones de terceros.

[220] Así, el Grupo de Trabajo 29 (2017) considera permitir el acceso a los datos personales, a través de una API accesible externamente que permita a sus titulares realizar solicitudes de datos posteriores,ya sea como una descarga completa u obteniendo, únicamente, los cambios desde la última descarga,sin que estas solicitudes adicionales sean onerosas para el responsable del tratamiento.

personales comprenda plenamente la definición, esquema y estructura de los datos personales que podría proporcionarle el responsable del tratamiento. Este debe proporcionar una perspectiva general de qué datos podrán ser portados, independientemente, de que se informe qué datos personales son tratados, ya que, como se ha dicho anteriormente, no todos los datos personales tratados son posibles de portar. Para ello, el Grupo de Trabajo 29 (2017) grafica algunos ejemplos como el proporcionar primero en un formato resumido, utilizando paneles de control que permitan al interesado portar subconjuntos de datos personales en lugar de la totalidad.

Adicionalmente, existe la preocupación de garantizar la seguridad en la transmisión de los datos personales. Ello implica el uso de cifrados y protocolos de seguridad de extremo a extremo en el envío, y el garantizar que los datos personales se entregan de forma segura a la persona correcta, para lo que también deben implementarse medidas de autenticación.

El Grupo de Trabajo 29 (2017) reconoce que los responsables del tratamiento deben evaluar los riesgos específicos relacionados con la portabilidad de los datos y adoptar las medidas adecuadas para su mitigación, como usar información adicional de autenticación (un secreto compartido o una contraseña de un solo uso, cuando el interesado deba ser autenticado); interrumpir o congelar la transmisión ante sospecha de interceptación de la cuenta; y, utilizar autenticación obligatoria basadas en token entre responsables del tratamiento.

3.3.4 Plazos aplicables

Debido a que el Proyecto de Ley (2021) no contempla plazo legal alguno, se analizarán primero los plazos dispuestos por algunas de las legislaciones extranjeras mencionadas anteriormente, para luego, proponer una opción adecuada en sede nacional.

Primero, en el caso de México, la LGPDPPSO (2017) dispone en su artículo 51° que la solicitud de portabilidad de datos personales deberá atenderse dentro

de 20 días extensible por 10 días más y en una sola ocasión, cuando se justifique y se notifique previamente al titular de los datos personales.

Segundo, en el caso argentino, su Proyecto de Ley N° 2896/20 dispone, de manera genérica que los derechos del titular de los datos, deberán ser atendidos en el plazo de diez (10) días hábiles de haberse intimado fehacientemente al responsable del tratamiento. Vencido el plazo, sin que se satisfaga el pedido o si a juicio del titular de los datos la respuesta se estima insuficiente, quedará expedito el trámite de protección de los datos personales ante la autoridad de control o podrá interponer la acción de habeas data.

Tercero, el RGPDP (2016) conforme a sus incisos 3 y 4 del artículo 12°, otorga un plazo de un mes a partir de la recepción de la solicitud, que puede ampliarse a un máximo de tres meses para casos complejos, siempre que se haya informado al titular de los datos personales los motivos dentro de dicho mes; en caso la solicitud fuera denegada, deberá informársele al solicitante acerca de las razones de tal negativa y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar las acciones judiciales pertinentes.

Sin embargo, el propio Grupo de Trabajo 29 (2017) reconoce que es "es probable que los responsables del tratamiento que gestionan servicios de la sociedad de la información estén mejor equipados para responder a las solicitudes en un plazo de tiempo muy corto". El simple hecho de que los datos personales estén siendo tratados solamente por medios automatizados facilita la gestión y control de los mismos. Aún más, si se implementan mecanismos que permiten seleccionar automáticamente aquellos datos personales, incluso por el propio titular de los datos personales, vía la extracción de los datos pertinentes y vía transferencia directa, como lo permiten las API o PIMS y otras iniciativasprivadas como el Data Transfer Project de Google y Facebook, como se mostró anteriormente.

Otra prueba del extenso plazo concedido por el legislador, es que Exposito-Rosso, Cao, Piquet, Medjaoui (s.f.) indican que el plazo del artículo 12° del RGPDP (2016) fue tratado con demasiada ligereza por el legislador, que no

sospechaba que los responsables del tratamiento de datos la utilizarían en su beneficio al utilizar esta extensión con demasiada facilidad. Así, ellos en su estudio afirman que describieron que los responsables del tratamiento de datos, cuando se vinculan con personas que conocen sus derechos y conocen los datos que pueden recuperar, siguen utilizando la prórroga del tiempo de respuesta como si se tratara de una solicitud de portabilidad más compleja. Lo anterior incluso cuando se trata de una solicitud de datos para un usuario normal que no está educado en la ley de datos personales.

Es decir, se dilata innecesariamente el plazo para responder a la solicitud de portabilidad cuando el responsable tiene los medios suficientes para responder antes y se extiende el plazo de dos (2) meses adicionales sin una justificación suficiente para ello. Esto, se da entre otros motivos, debido a la poca supervisión y coerción existente por parte de las autoridades de control.

De vuelta al panorama nacional, el artículo 55.3° del Reglamento (2013) sostiene que tratándose del ejercicio de los otros derechos como los de rectificación, cancelación u oposición, el plazo máximo de respuesta del titular del banco de datos personales o responsable del tratamiento será de diez (10) días contados desde el día siguiente de la presentación de la solicitud correspondiente.

Si la información proporcionada en la solicitud resulta insuficiente o errónea de forma que no permita su atención, el artículo 56° indica que el titular del banco de datos personales podría requerir, dentro de los siete (7) días siguientes de recibida la solicitud, la documentación adicional al titular de los datos personales. Esta deberá ser presentada en un plazo de diez (10) días, desde el día siguiente de la recepción del requerimiento sino se tendrá por no presentada la solicitud. Igualmente, conforme al artículo 57°, dichos previstos para la respuesta y/o la atención de la solicitud de portabilidad podrán ser ampliados una sola vez, y por un plazo igual, como máximo, siempre y cuando las circunstancias lo justifiquen, debiendo comunicársela al titular del dato personal dentro del plazo que se pretenda ampliar.

Con ello, consideramos que el plazo general previsto por el artículo 55.3° y demás condiciones de los artículos 56° y 57° resultan aplicables, suficientes y adecuadas para la incorporación del derecho a la portabilidad de datos personales; no habiendo necesidad de configurar un plazo específico, ni, mucho menos, uno mayor a efectos de evitar la dilación en la atención de solicitudes a los titulares de los datos personales, como sucede en algunos casos de la legislación comparada.

3.3.5 ¿Qué derechos y obligaciones específicos implica?

Puccinelli (2017) indica que, con base en la experiencia europea (RGPDP y Grupo de Trabajo 29), la mexicana (LGPDPPSO) y los "Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales" ya aprobados por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018), haciendo la salvedad que el primero aplica al sector privado mientras que el segundo no, resulta pertinente mencionar los siguientes derechos del titular de los datos personales con respecto al derecho a la portabilidad de datos personales:

- Derecho a recibir del responsable del tratamiento de los datos personales requeridos, de manera gratuita, sin dilaciones indebidas y en un formato estandarizado que permita la interoperabilidad: primero, la gratuidad debe aplicar a toda comunicación y acción realizada salvo si las solicitudes son manifiestamente infundadas, excesivas o repetitivas, pudiendo cobrar un canon o tarifa razonable o negarse justificadamente a proporcionarlo.

- Segundo el RGPDP (2016) dispone que el responsable del tratamiento, deberá proporcionar una visión general de forma concisa, transparente, inteligible y fácilmente accesible, usando un lenguaje claro y sencillo. Esto aplica incluso ante la presencia de gran número de datos personales o de existir una estructura compleja u otros problemas técnicos, debiéndose proporcionar sin dilaciones indebidas y de modo que se permita su reutilización, los datos personales. Lo anterior "implica que el formato debe ser interoperable, aunque esto no crea la obligación para los responsables del tratamiento de adoptar o mantener sistemas de tratamiento que sean

técnicamente compatibles" (p. 223). Tercero, el autor coincide en que, al no definirse el formato expreso en el RGPDP (2016) y, dado que existirá diferencias entre los diversos sectores, requiere que las partes interesadas del sector y asociaciones comerciales trabajen conjuntamente sobre una serie común de normas y formatos interoperables.

- Derechos a obtener los datos personales para almacenarlos y que se transmitan de un responsable del tratamiento a otro sin impedimentos: Según Puccinelli (2017), significa que debe haber una acción por parte del responsable del tratamiento a ayudar o facilitar a los titulares del tratamiento, el almacenamiento seguro de sus datos personales en los sistemas propios al momento de entregárselas. Esto implica recomendarles formatos apropiados, medidas de cifrado y trasmitirlos sin trabas indebidas ya sea al titular de los mismos o al tercero que este último designe.

- Ejercicio del derecho a la portabilidad de datos sin perjuicio de los demás derechos existentes: este puede ejercerse independientemente de cancelar los datos personales o de seguir usando los servicios del responsable del tratamiento, aun después de haberse portado los datos personales. Tampoco, podrá conllevar automáticamente el borrado de los datos personales del sistema del cual se porten, salvo que el titular de los datos personales estuviese finalizando la relación con el responsable del tratamiento y, así, lo solicitase. De igual manera, si tras ejercer la portabilidad, el titular de los datos personales considerase que tales datos no responden plenamente a su solicitud podrá ejercer el derecho de acceso, a efectos de verificar si la información que se transfirió era la correspondiente, en el marco del ejercicio del derecho a la portabilidad.

- Derecho a que no se extienda el periodo de retención bajo la excusa del ejercicio del derecho a la portabilidad: Puccinelli (2017) y el Grupo de Trabajo 29 (2017) indican que el ejercicio del derecho a la portabilidad no es justificación válida para rechazar el pedido de cancelación de los datos ni extender la duración del almacenamiento aplicable a los datos personales.

De igual manera, con base a lo expresado por Puccinelli (2017), deben considerarse los siguientes deberes específicos aplicables tanto a los responsables del tratamiento cuando sean emisores como receptores de los datos personales portados:

- Deber de informar a los interesados acerca de la disponibilidad del nuevo derecho a la portabilidad: como parte del deber de información previsto en el artículo 18° de la LPDP (2011), que indica que "el titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación" sobre "la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello". En ese sentido, deberá informarse sobre la incorporación de la posibilidad de ejercer el derecho a la portabilidad. Lo anterior se da en aquellos tratamientos que se encuentren en curso y los que estén recién iniciándose. Cabe mencionar que el Grupo de Trabajo 29 (2017) recomienda que este derecho sea recordado, con especial antelación al cierre de cualquier cuenta, junto con los tipos de datos que su titular podrá recibir usando tanto el derecho a la portabilidad, como el derecho de acceso. Resultaría acertado tomar esto en cuenta en sede nacional.

- Deber de transmitir los datos personales con seguridad y autenticando debidamente al solicitante como al receptor: Puccinelli (2017) recuerda que, al amparo del RGPDP (2016), debe garantizarse "la seguridad adecuada de los datos personales, incluyendo la protección contra tratamientos no autorizados o ilícitos y contra su pérdida accidental, destrucción o daños, utilizando medios técnicos y organizativos apropiados" (p. 225). Para ello, puede emplearse el cifrado en el envío y mecanismos de autenticación para verificar la identidad tanto del solicitante como del destinario correcto, costos que no deberán ser trasladados al titular de los datos personales. Para la autenticación del titular de los datos personales, en caso se hubiera realizado previamente, al inicio del tratamiento y, por ello, no existiese duda al respecto, no debería volverse a autenticarse innecesariamente; si, por el

contrario, este resultase imposible de identificar o se requiere de información adicional por dudas razonables, como cuando la información está vinculada a seudónimos o identificadores exclusivos, podrán implementarse procedimientos apropiados de autenticación.

Adicionalmente, podría resultar idóneo revisar algunas herramientas en materia de protección de datos personales, como la "Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales", aprobada por la Resolución Directoral Nº 019-2013-JUS/DGPDP. Este es un instrumento que facilita el cumplimiento de la LPDP (2011) a efectos de actualizar dichas disposiciones a las nuevas normas ISO e incorporarnuevos supuestos con respecto al tratamiento automatizado y transferencias nacionales e internaciones, en virtud del cumplimiento del derecho a la portabilidad de datos personales que se pretende incorporar.

- Deber de limitarse a proveer datos personales que incumban al interesado sin afectar negativamente a los derechos y libertades de terceros: no deben transferirse datos personales de terceros, anónimos o pseudonimizados (disociados, salvo que tales seudónimos estén claramente ligados a un interesado) o que no hayan sido proporcionados por este.

  El Grupo de Trabajo 29 (2017) indica que tal interpretación no será excesivamente restrictiva cuando la información contiene datos personales referidos a varios interesados que no han dado su consentimiento, como registros telefónicos con detalles de llamadas de terceros; se requiereevaluar los datos facilitados por el titular de los datos personales, incluido los datos observados durante actividades (como un historial de transacciones o registro de accesos); y, se necesite valorar qué datos fueron recabados mediante el seguimiento y registro del titular de los datos personales, abarcando aquellos transmitidos o no de manera activa o consciente (por ejemplo, una aplicación registrando el ritmo cardiaco o pararastrear hábitos de navegación).

Puccinelli (2017) indica que se afectarán los derechos y libertades de terceros, si, por ejemplo, una transmisión impidiese a terceros ejercer sus derechos o los afecta lesionando secretos comerciales o de propiedad intelectual. Por ello, si se incluyen datos personales de terceros en el ejercicio del derecho a la portabilidad, debería señalarse otro motivo de la legalidad del tratamiento como podría ser un interés legítimo del responsable receptor de los datos o la utilización ulterior para una actividad puramente personal o doméstica.

En la legislación peruana, esto es analógico o paralelo, por un lado, a los supuestos de excepción a la obtención del consentimiento contemplados en el artículo 14° de la LPDP (2011). Con respecto a la excepción al ámbito de aplicación de la LPDP (2011) del artículo 3.1°, se indica que las disposiciones de estas no se aplican a los datos personales "contenidos o destinados a ser contenidos en bancos de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar".

Finalmente, resulta relevante la posibilidad de promover en los servicios digitales, herramientas que permitan seleccionar los datos que consideren relevantes y excluir, donde proceda, otros datos que no se deseen portar; y, habilitar mecanismos de autorización para que otros titulares de los datos personales involucrados puedan brindar su consentimiento y, así, facilitar la transmisión de datos personales, si así lo desean (por ejemplo, en una foto conjunta, foro, chats, etc.).

- Deber de omitir retener los datos personales: los datos personales no podrán ser retenidos o almacenados por mayor tiempo al necesario legalmente o para el cual el titular de los datos personales otorgó su consentimiento. De igual manera, el receptor de los datos personales, al convertirse en nuevo responsable del tratamiento, requerirá omitir la retención de datos irrelevantes para el servicio que se prestará, debiendo proceder a su eliminación inmediata.

- Deber de ofrecer diferentes opciones de puesta en práctica del derecho: Puccinelli (2017), acertadamente, rescata que, para cumplir con este derecho, resulta idóneo contar con un menú de opciones, en la medida de lo posible, con procedimientos de respuesta automática y que contenga botones de selección para que el titular de los datos personales pueda identificar aquellos datos que desea (ya sea por rango de fecha u otros criterios de búsqueda y el formato en el que se portarán). Así, de acuerdo a su conveniencia, decida si desea la descarga directa (también llamado *download as solution*, mediante un botón de descarga) o, por el contrario, transmitirla directamente a otro responsable (lo que se lograría, por ejemplo, poniendo a disposición una API).

- Deber de los receptores de los datos portados de informar sobre la naturaleza de los datos personales que sean relevantes para la ejecución de sus servicios y garantizar que tales datos sean pertinentes y no excesivos en relación con el nuevo tratamiento de datos: conforme al deber de información y al principio de finalidad, legalidad, consentimiento y proporcionalidad, todo nuevo tratamiento de los datos personales debe ser acorde a la LPDP (2011) y demás disposiciones aplicables. Por ello, el responsable receptor de los datos personales debe informar oportunamente, es decir, con anterioridad a su recepción, qué datos personales son los necesarios para el tratamiento a realizarse y/o ejecución de sus servicios. Esto permitirá limitar los riesgos y reducir la transmisión de datos personales innecesarios.

3.3.6 ¿Qué actuaciones y/o medidas por parte de la Dirección de Protección de Datos Personales deberían esperarse?

El proceso de portabilidad de datos en otras legislaciones, como el RGPDP (2016), que es el pionero y el que más medidas ha adoptado para su implementación, ha demostrado ser complejo y en algunos casos hasta "una barrera para acceder y utilizar los datos propios por parte de los titulares de los datos personales" (Exposito-Rosso, Cao, Piquet, Medjaoui, s.f.).

Por tanto, es esencial centrarse en la experiencia del titular de los datos personales, como usuario del servicio, en virtud del cual se traten los datos. Para

ello, las recomendaciones sobre el diseño y flujos de usuarios, sobre cómo manejar las solicitudes de portabilidad de datos a los responsables del tratamiento en el sector privado, puede ser una actuación orientativa de gran ayuda por parte de la autoridad.

De igual manera, como sucede con el ejercicio de la portabilidad numérica en el servicio público móvil y telefonía fija en Perú por parte de OSIPTEL, la Autoridad Nacional de Protección de Datos Personales también podría coadyuvar en la implementación de este derecho de muchas formas, mediante secciones informativas en su portal web sobre el contenido y mecanismos de ejercicio existente del derecho a la portabilidad de datos personales. Esto lo hace OSIPTEL[221] y cualquier otro mecanismo que coadyuve a la implementación y fortalecimiento del derecho a la portabilidad de los datos personales en el sector privado, como charlas, absolución de consultas, opiniones públicas o boletines informativos como suele publicar en su sitio web[222].

Cabe preguntar si es necesario implementarse un registro admnistrativo a cargo de la Autoridad Nacional de Protección de Datos Personales similar a la denominda "Base de Datos Centralizada Principal" de titularidad de OSIPTEL. Así, según el artículo 2.6° del Texto Único Ordenado del Reglamento de Portabilidad Numérica en el Servicio Público Móvil y el Servicio de Telefonía, aprobado mediante Resolucion de Consejo Directivo Nº 286-2018-CD-OSIPTEL, tal registro contiene la información actualizada correspondiente a la portabilidad en el servicio público móvil y en el servicio de telefonía fija y con ello el registro de las solicitudes de portabilidad[223]; es decir, administra todas las solicitudes de

---

221 Para mayor información ver: https://www.osiptel.gob.pe/portal-del-usuario/preguntas-frecuentes/portabilidad-numerica

222 Para mayor información ver: https://www.gob.pe/busquedas?contenido%5B%5D=publicaciones&institucion%5B%5D=anpd&sort_by=recent

223 Ello, a su vez, le permite al OSIPTEL medir y analizar el impacto de la portabilidad numérica en el sector. Para ello emite reportes periódicos analizando la desconcentración y migraciones de proveedores de telefonía móvil y fija. Esta idea va ligada a evitar los efectos *lock-in*, que se

portabilidad realizadas en el sector. Al respecto, se considera que esta medida, en materia de datos personales, resultaría innecesario para los privados y hasta para la propia Autoridad Nacional de Protección de Datos Personales, en tanto que la portabilidad numérica opera a un solo sector específico como lo es la telefonía y, además, es un servicio público.

Por el contrario, los responsables del tratamiento que manejen datos personales por medios automatizados, lo harán en incontables sectores de la industria. Por ello, la fiscalización resultaría onerosa y haría incurrir en mayores gastos a la administración pública. Además, es de acotar que muchas legislaciones, al incorporar este derecho, evitan imponer restricciones para su cumplimiento porque buscan que cada sector de la industria y responsable del tratamiento, implemente los mecanismos más idóneos para el cumplimiento de dicho deber: y, así buscar promover consensos, estandarización e incluso fomentar la innovación y digitalización en las distintas industrias como consecuencia del consenso y comunicación generado para las transferencias entre responsables al ejecutar la portabilidad de datos personales.

Por supuesto, ello no impide que la autoridad pueda medir de otras maneras el cumplimiento del derecho a la portabilidad de datos personales, como lo sucede con otros derechos al momento de realizar fiscalizaciones, ya sea de oficio o por motivos de denuncias dentro de sus funciones y competencias existentes.

Seguidamente, en caso de incorporarse este derecho en la normativa, podría surgir la interrogante sobre si al portar los datos personales, ya sea al propio titular o a cualquier otro tercero que este designe, debería implicar una transferencia nacional e internacional. Ante ello, se requeriría consecuentemente declarar

---

mencionaron anteriormente, y que el abonado-usuario pueda cambiar libremente de proveedor, si así lo desea. Para mayor información ver:

- https://www.osiptel.gob.pe/portal-del-usuario/noticias/peru-portabilidad-numerica-en-telefonia-movil-crecio-27-25-en-los-ultimos-tres-meses/
- https://repositorio.osiptel.gob.pe/handle/20.500.12630/258/recent-submissions?offset=40

ambas posibilidades ante el Registro Nacional de Protección de Datos Personales. Si bien el cumplimiento de dicho derecho sí implicará una transferencia[224] nacional y/o internacional[225], dependiendo donde se ubique el receptor de los datosportados, se encuentra exceptuado del segundo párrafo del artículo 15° que sostiene que "[e]n caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debegarantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto [por la LPDP]".

Esto en tanto que la portabilidad se ejerce en virtud de una solicitud (en ejercicio de su derecho) del titular de los datos personales. Ello no es exacto con lo expresado en el numeral 7 del artículo 15º, ya que dicho numeral es concebido para cuando se cuente con consentimiento para el tratamiento solicitado por el responsable. Además, el numeral 8 siguiente de dicho artículo indica que también procede en caso de "otros que establezca el reglamento de la presente Ley, con sujeción a lo dispuesto en el artículo 12°", siendo que, por vía reglamentaria, debería precisarse, para evitar confusión o interpretaciones alejadas, que el ejercicio del derecho a la portabilidad de datos personales constituye una excepción a lo dispuesto en el segundo párrafo del artículo 15° de la LPDP (2011).

---

[224] Ello en tanto que el artículo 2.18º de la LPDP (2011) dispone que es lo siguiente:

> Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales.
>
> 4. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, incluyendo lo necesario para actividades como la autentificación de usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta y aquellas actividadesque el manejo de la relación contractual requiera.

[225] Ello, en tanto el artículo 2.10º de la LPDP (2011) indica que el flujo transfronterizo es toda transferencia al extranjero de los datos personales "a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los mediospor los cuales se efectuó la transferencia ni el tratamiento que reciban.

Respecto a si se debe o no declarar como transferencia nacional o flujo transfronterizo ante el Registro Nacional de Protección de Datos Personales, se debe precisar que, en tanto existe la posibilidad de que los titulares ejerciten sus derechos de portabilidad en cualquier momento y, en principio, cuando sea técnicamente posible, a cualquier destino del mundo, no debería ser exigible declararlo. Ello debido a que ambas secciones, dentro del "Formulario de Inscripción de Banco de Datos Personales" denominadas "III. Transferencias de datos personales a nivel nacional" y "iv. transferencias de datos personales a nivel internacional (flujo transfronterizo)", respectivamente, fueron concebidas para las transferencias que el titular realiza en virtud del tratamiento para el cual obtuvo consentimiento y/o informa al encontrarse exceptuado conforme al artículo 14°.

Además, en el caso de ingresar cada destinario, resultaría imposible el saber con anticipación quiénes serían los receptores exactos o, peor aún, declararlos constantemente sería engorroso, sobre todo en el caso específico del flujo transfronterizo, indicando los países y los receptores de los datos personales con la información que, a la fecha, es solicitada (país, documento de identidad, entidad receptora o importadora, operación). Podría colocarse en ambas opciones que la finalidad de ambas transferencias será exclusivamente cumplir con las solicitudes de portabilidad de datos personales que se requieran y, en el caso de la categoría de los receptores, indicar "otros" especificando que son el titular de los datos personales o el tercero que él, conforme al procedimiento legal previsto, designe.

Por último, a efectos de poder implementar este derecho, resultaría idóneo brindar un plazo de adecuación a las modificaciones normativas que se introduzcan. La LPDP (2011) , publicada el 3 de julio de 2011, otorgó un plazo amplio y gradual de adecuación que culminaría, luego de los dos (2) años de la promulgación de su Reglamento (2013), conforme a la Primera Disposición Complementaria Transitoria de dicho Reglamento (2013). De igual manera, en la Unión Europea, el RGPDP (2016) otorgó un plazo amplio, desde el 24 de mayo de 2016 hasta su aplicación el 25 de mayo de 2018; no obstante, el RGPDP (2016) si suponía un cambio sustancial en todo el régimen de protección de datos personales pasando de su directiva anterior al presente reglamento.

Un plazo así de amplio no sería necesario ni conveniente en tanto que las modificaciones propuestas en esta investigación para la implementación del derecho a la portabilidad de datos no supongan una modificación total o sustancial del régimen de protección de datos personales vigente. Por el contrario, las modificaciones propuestas buscan la incorporación de un nuevo derecho junto con los mecanismos necesarios y adecuados. Para ello, además, se propone una implementación muy flexible en todos los sentidos, como buscar consensos con los actores involucrados en cada sector de la industria; evitar imponer estándares legales que limiten la innovación, dando solo lineamientos que deben ser cumplidos por los responsables del tratamiento; y, brindar libertad para los mecanismos y vías técnicas de atención y ejercicio a este derecho.

Por ello, otorgar un plazo máximo de un (1) año, contado desde su publicación en el Diario Oficial "El Peruano" para culminar la adecuación resulta suficientemente extenso y comprensible a todos los sectores de la industria para que puedan ir implementando: mecanismos que permitan portar la data al titular de los datos personales y, con respecto a las partes interesadas del sector y asociaciones comerciales, puedan ir acordando conjuntamente una serie común de normas y formatos interoperables que permitan hacer "técnicamente posible" la transferencia directa de los datos personales entre responsables de cada sector e, incluso, entre diferentes sectores de la industria digital.

Conclusiones

1. Los datos son materia prima y activos clave. Tienen una naturaleza representativa y perceptible por el ser humano y otras herramientas tecnológicas. Poseen una inherente falta de neutralidad en tanto reflejan elecciones sobre quién o qué los genera e interpreta. Todo es, contiene o genera datos que, al interpretarse, derivan en "significado" que es un valor agregado al que se le denomina "información"; por ello, todos los datos tienen un significado potencial inagotable. El constante tratamiento de la información generará ulteriormente el "conocimiento". Estas tres (3) distinciones inciden tanto en la práctica comercial como en el ordenamiento jurídico, sobre todo, en el régimen de protección de datos personales.

2. Todo régimen de protección de datos personales considera una dicotomía de intereses involucrados. Por un lado, la privacidad y otros derechos fundamentales asociados; y, por el otro, a la economía y el mercado. Hallar un balance de ambos enfoques es lo idóneo, como el otorgar derechos a los titulares de los datos personales que estén en equilibrio con los objetivos económicos, generando confianza en dicho tratamiento.

3. Doctrinariamente, cuatro (4) elementos componen un dato personal: información, identificabilidad, relativo a alguien y su vinculación a una persona natural. Estos han sido reconocidos administrativamente en una peculiar mezcla "que se trate de información personal" y "que se trate de una información que permita identificar o hacer identificable al titular del derecho". Además, la definición legal del dato personal es binaria, abstracta, abierta, enumerativa y "a la inversa", en tanto que solo si el dato revela información personal, este también lo será. Ello colisiona con la naturaleza dinámica de los datos y herramientas, como el Big Data y IoT que impactan directa y fácilmente en los individuos, lo que propicia zonas grises de desprotección a los titulares de los datos personales.

4. El derecho a la protección de los datos personales o la autodeterminación informativa es una manifestación del derecho a la personalidad que contempla

mecanismos de control cuando los datos personales son objeto de tratamiento. Este posee una función habilitadora o facilitadora de otros derechos fundamentales; por ende, es distinto y más amplio que el derecho a la privacidad. Si bien, constitucionalmente, se reconoce que tal derecho comprende el hacer uso de la información privada y, por ende, obtener copia de ella, resulta necesaria una vía legal específica que contemple (i) el portar los datos personales en entornos digitales, garantizando su reutilización; y, (ii) vías que delimiten el cumplimiento de las condiciones técnicas para garantizar una adecuada portabilidad en el entorno digital.

5. Si bien el derecho de acceso también comprende usar la información propia y obtener copia de esta. No resulta la vía legal adecuada, en tanto el Reglamento (2013) impone que la atención de tal derecho deberá ser "en formato claro, legible e inteligible, sin utilizar claves o códigos que requieran de dispositivos mecánicos para su adecuada comprensión" y en "lenguaje accesible al conocimiento medio de la población y de los términos que se utilicen". Si bien se permite que la entrega de la información solicitada en virtud del derecho de acceso sea vía electrónica o automatizada, como archivos Word, PDF u otros comúnmente usados, sean legibles al conocimiento medio de la población, no garantizan la reutilización directa de la información contenida. Al contrario, formatos que sí permitirían la reutilización no son fácilmente entendibles por una persona, pues su contenido no es texto plano. Por ello, el entregar información en formatos "reutilizables", en el entorno digital, supera los límites del derecho de acceso.

6. El derecho a la portabilidad, más que "relacionarse", subyace al derecho de acceso siendo una "expresión" o "actualización" del inminente fenómeno de digitalización frente a las limitaciones del derecho acceso en entornos digitales. Para brindar mayor autonomía y promover su implementación, varias legislaciones lo han incorporado como un derecho nuevo e independiente. Por ello, debe ser incorporado como un artículo independiente o, al menos, dentro de la sección correspondiente al derecho al acceso siempre y cuando se haga hincapié en que este derecho es independiente al derecho de acceso, pues responde a particularidades y necesidades distintas. Con ello, se evitarán confusiones por parte de los administrados y de la propia autoridad al ponerlo en práctica.

Introducir el derecho a la portabilidad de datos personales puede generar implicancias económicas positivas. Por un lado, el acceso a los datos es un factor competitivo vital en el sector digital; y, por el otro, la privacidad y protección de los datos personales es cada vez más un parámetro competitivo al elegir servicios. Al asentar los derechos personales de los individuos y reafirmarse el control del titular de los datos personales sobre sus datos personales, garantizando su reutilización en el entorno digital, la portabilidad de los datos representa una oportunidad para reequilibrar la relación entre los interesados y los responsables del tratamiento. De ahí, se analiza su incidencia en las relaciones de consumo digital. Así, para los consumidores, se reducirían los costos de cambio y aumentaría el bienestar del consumidor.

Lo anterior puede contribuir a la competencia entre los servicios digitales al facilitar y promover el cambio de servicio y el uso de datos personales en la industria. Esto impacta en agentes nuevos y/o con menores cuotas de mercado, al aminorar tangencialmente las barreras de entrada e incentivar la innovación al coadyuvar el problema del "arranque en frío". Esto se evidenció en el *Open Banking* con la aparición de nuevos servicios *fintech*, tras la disponibilidad de diversas API que posibilitaron la portabilidad continua de datos y el desarrollo de servicios complementarios.

No obstante, debe evitarse, con adecuadas medidas regulatorias, que se promuevan incentivos perversos para tratamientos desproporcionados que, colateralmente, reduzcan los estándares de calidad en protección de datos personales, privacidad y, con ello, el bienestar del consumidor. Adicionalmente, debe advertirse que el derecho a la portabilidad no resulta una solución o, al menos, un paliativo frente a otros efectos negativos del mercado digital, como lo son los efectos de red. Estos probablemente persistirán, pese a su introducción, pues gran parte del valor del servicio de una plataforma depende de la cantidad de usuarios, generando un "bloqueo" al cambio de proveedor. Para lidiar con ello, sí se requeriría mayor grado de interoperabilidad desde el protocolo para que los usuarios puedan interactuar desde diferentes plataformas. Esto sucede en el sector de las telecomunicaciones, donde pueden comunicarse y migrar sin importar el operador contratado. Sin embargo, tal propuesta escapa del ámbito de la

protección de datos personales y generaría otras implicancias como la necesidad de supervisión estatal, pudiendo además provocar riesgos colaterales como barreras de entrada y de innovación ante los mayores estándares de interoperabilidad que se tendrían que imponer al mercado en vía regulatoria.

7. La portabilidad de datos personales es también vista en el marco internacional como un enfoque de política pública para mejorar el acceso e intercambio de datos y la reutilización de datos en el sector privado y entorno digital, habiendo otras legislaciones y áreas del derecho desde las que se pueden implementar medidas análogas o similares que sirven de experiencia y medidas conexas para su fortalecimiento. La portabilidad de datos personales requiere (i) interoperabilidad a nivel de los datos, sobre todo, para permitir un acceso continuo y potencialmente en tiempo real a los mismos; y, la (ii) la necesidad de generar consensos y colaboración entre agentes del mercado para poder materializarse, es decir, lograr estandarización sobre aspectos técnicos en la cadena de valor de los datos personales sobre sus atributos, terminología, estructura, organización, almacenamiento (ubicación), lectura, uso, protocolos para su portabilidad, abordándose los riesgos semánticos y sintácticos en su compatibilización.

   A la fecha existen modelos técnicos implementados que permiten ejecutar el derecho a la portabilidad de datos, tanto para su exportación por el titular de los datos personales, como directamente entre responsables del tratamiento. En ambas, se evidencia que el uso de API se ha vuelto un estándar de facto tanto en origen, como en destino para transferencias entre responsables; no obstante, las infraestructuras de las API requieren estandarización para garantizar, en última instancia, que la data portada pueda ser reutilizada y las API de distintos responsables del tratamiento puedan interoperar cuando se requiera y sin ninguna contingencia. Finalmente, existen múltiples innovaciones y tendencias, en distintos estados de desarrollo, hacia la generación de herramientas que permitan otorgar un mayor control y empoderando a los titulares de los datos personales sobre sus datos (no solo personales) en el entorno digital. Sin embargo, dichas iniciativas requieren ser respaldadas y promovidas para que sigan mejorando y ganando mayor presencia en el mercado, siendo que, la portabilidad de datos personales, va alineado a dicho objetivo.

8. El derecho a la portabilidad de datos personales debe estipular las siguientes características específicas en su fórmula legislativa:
    - Respecto al tipo de almacenamiento y fuentes de obtención de los datos personales, debe comprenderse a los medios automatizados interpretándose de una manera amplia y no restrictiva (lo que comprende, a su vez, la vía electrónica), siempre que sea técnicamente posible cumplir con el almacenamiento de los datos personales en los formatos y esquemas requeridos. Así, sobre las fuentes de obtención de los datos personales, no deben estipularse mayores limitaciones como las pretendidas en el Proyecto de Ley, debiéndose entender ampliamente en tanto el tratamiento se realice por cualquier medio automatizado.
    - Resultaría deseable que, para extender los efectos de este derecho, sea aplicado indistintamente al sector privado como público; sin embargo, resulta prioritario su introducción en el sector privado.
    - Los motivos de improcedencia deberán ser cuando (i) no fuese técnicamente posible la transferencia, lo que incluye que su ejercicio imponga una carga financiera, técnica excesiva o irrazonable al responsable o encargado del tratamiento; (ii) vulnere la protección de derechos de terceros; (iii) obstaculice las actuaciones judiciales o administrativas en curso; y, (iv) otras excepciones legales.
    - Los tipos de datos personales aplicables deberían ser (i) todos aquellos datos personales otorgados directa e indirectamente por su titular, es decir, incluir a los datos observados y a los datos en bruto generados en la recolección; (ii) los datos derivados e inferidos como una buena práctica comercial siempre que no se genere ninguna vulneración de terceros, es decir, que se respeten los derechos de propiedad intelectual y secreto comercial, teniendo en cuenta que un "posible riesgo empresarial", en sí mismo, no debería considerarse una negativa justificada para no incluir tales datos personales en la solicitud de portabilidad; (iii) los datos anonimizados no deberían incluirse, pero sí aquellos datos personales que fueron disociados, en tanto se encuentren claramente vinculados con su titular; y, (iv) los datos personales con o sobre otros terceros, no deberían hacerse una interpretación excesivamente restrictiva, permitiendo portar los datos que

incumban a su titular, pero tomando en cuenta que el nuevo responsable no deberá tratarlos para fines que afecten negativamente derechos y libertades de terceros. También, resulta deseable promover la implementación de herramientas que permitan recabar el consentimiento informado, libre, previo expreso e inequívoco de aquellos otros titulares de datos personales, en caso deseen permitir que sus datos personales involucrados sean portados por el solicitante de la portabilidad de sus datos personales.

- El formato en el que deben proporcionarse los datos personales debe ser uno estructurado, de uso común y lectura mecánico que permita su reutilización directa. Por ello, resulta deseable promover la creación y uso de formatos interoperables con otros sistemas informáticos, que tengan un elevado nivel de abstracción. Ejemplo de ello son los formatos abiertos en los que se pueda incluir los metadatos y se precise el significado de la información intercambiada. Debiendose contar con la cooperación de las partes interesadas en los sectores allegados para generar consensos comune en la industria digital.
- Debe estipularse el plazo máximo de un (1) año, desde la publicación de la modificación legislativa para culminar la adecuación de los responsables del tratamiento con respecto a implementar: (i) mecanismos que permitan portar la data al titular de los datos personales y (ii) fomentar a las partes interesadas del sector y asociaciones comerciales alcanzar conjuntamente normas y formatos interoperables comunes que permitan hacer técnicamente posible la transferencia directa de los datos personales entre responsables de cada sector e, incluso, de diferentes sectores de la industria digital.

9. Deben observarse las siguientes consideraciones por vía regulatoria y/u orientativa para el ejercicio del derecho a la portabilidad de datos personales:
    - Su ejercicio será de carácter gratuito, salvo que se establezca lo contrario en normas especiales de la materia. Ni los costos de implementación de los canales, procesos o vías para la atención del derecho a la portabilidad de datos personales, ni otras solicitudes previas deberían ser cobrados al titular

de los datos personales. El cobro de un canon o tarifa adicional se tendrá que justificar solo si implica un costo adicional.

- Se deberán observar los requisitos del artículo 50º del Reglamento (2013) para la solicitud de ejercicio y acreditándose de la siguiente manera:
  (i) Nombres y apellidos del titular del derecho y, en caso de su representante, lo que se logra mediante la autenticación.
  (ii) Petición concreta de los datos personales a ser portados, es decir, dando detalle si se desea obtener una copia de los datos personales para sí mismo y/o transmitirlos directamente a otro responsable del tratamiento.
  (iii) Domicilio entendida como dirección electrónica para recepcionar la solicitud de portabilidad del titular de los datos personales o al tercero que designe brindando suficientes detalles de la identidad del receptor a efectos de poder validar que ese el destinario indicado: (i) si es a otra persona natural, su nombre completo, DNI u otro documento de identidad y alguna vía de contacto adecuada para entablar la comunicación y transmisión de los datos (por ejemplo, correo electrónico, cuenta de alguna red social, o hasta dirección física); y, (ii) si es a una persona jurídica, razón/denominación social y No. RUC o código de identificación tributaria, cuando no pueda ponerse en contacto directamente. En algunos casos de transferencia a terceros proveedores de servicios digitales, no resultará necesario brindar detalles como la razón social o un código de identificación tributaria, sino que otros mecanismos más sencillos o directos, como el url del sitio web o de la cuenta del titular de los datos personales en dicho servicio digital (red social, correo electrónico, etc.), sería suficiente para saber con certeza a quién y donde transferir.
  (iv) Fecha y firma del solicitante, pudiendo ser cualquier otra constancia que permita acreditar la realización de su solicitud y la fecha en que se realiza.
- Debe observarse el plazo general previsto por el artículo 55.3º y demás condiciones de los artículos 56º y 57º del Reglamento (2013) para atender y dar respuesta a la solicitud de ejercicio de tal derecho.

- Debe precisarse para evitar confusión o interpretaciones alejadas, que el ejercicio del derecho a la portabilidad de datos personales constituye una excepción a lo dispuesto en el segundo párrafo del artículo 15º de la LPDP (2011).
- Deben implementarse adecuadas medidas técnicas, legales y organizativas para garantizar la seguridad y confidencialidad en la transmisión de los datos personales, implementando (i) el uso de cifrados y protocolos de seguridad de extremo a extremo en el envío; y, (ii) el garantizar que los datos personales se entregan de forma segura a la persona correcta con adecuadas medidas de autenticación. Asimismo, existe la obligación de evaluar los riesgos específicos relacionados con la portabilidad de los datos y adoptar las medidas adecuadas para su mitigación, (i) usando información adicional de autenticación (un secreto compartido o una contraseña de un solo uso, cuando el interesado deba ser autenticado); (ii) interrumpir o congelar la transmisión ante sospecha de interceptación de la cuenta; y, (iii) utilizar autenticación obligatoria basadas en *tokens* entre responsables del tratamiento.

10. El derecho a la portabilidad de datos personales conlleva los siguientes derechos específicos a sus titulares: (i) recibir del responsable del tratamiento los datos personales requeridos, de manera gratuita, sin dilaciones indebidas y en un formato estandarizado que permita la interoperabilidad del formato y los datos; (ii) obtener los datos personales para almacenarlos y que se transmitan de un responsable del tratamiento a otro sin impedimentos; (iii) ejercerlo sin perjuicio de los demás derechos existentes, lo que también implica que el titular de los datos personales deberá comprender plenamente la definición, esquema y estructura de los datos personales que podrá proporcionarle el responsable del tratamiento para lo que este debe proporcionar una perspectiva general de qué datos podrán ser portados. Como contracara, conlleva las siguientes obligaciones a los responsables del tratamiento ante quienes se ejerza (como destinatarios y receptores): (i) informar a los interesados acerca de la disponibilidad del nuevo derecho a la portabilidad; (ii) transmitir los datos personales con seguridad y autenticando debidamente al solicitante como al receptor; (iii) proveer únicamente datos personales que incumban al interesado sin afectar

negativamente a los derechos y libertades de terceros; (iv) omitir retener los datos personales o almacenarlos por mayor tiempo al necesario legalmente o para el cual el titular de los datos personales otorgó su consentimiento; (v) ofrecer diferentes opciones de puesta en práctica del derecho; (vi) los receptores de los datos portados de informar sobre la naturaleza de los datos personales que sean relevantes para la ejecución de sus servicios y de garantizar que tales datos sean pertinentes y no excesivos en relación con el nuevo tratamiento de datos.

11. En cuanto al Registro Nacional de Protección de Datos Personales, no resulta necesario o idóneo crear un registro de portabilidad ni ejercicio del mismo. Asimismo, con respecto a si debería declararse como una transferencia nacional o internacional, podría incorporarse una sección en la que se indique si a cada titular del banco de datos personales le "es técnicamente posible transferir directamente datos personales a terceros en ejercicio al derecho a la portabilidad" porque cuenta con mecanismos implementados para ello, debiendo especificarse en un recuadro conexo qué mecanismos son esos (por ejemplo, API u otros) a efectos de tener mayor visibilidad y uniformidad en la adecuación de este derecho.

Bibliografía

Doctrina

Abrams, M. (2014). The Origins of Personal Data and its Implications for Governance, *The Information* *Accountability Foundation.* http://dx.doi.org/10.2139/ssrn.2510927

Agencia de los Derechos Fundamentales de la Unión Europea [FRA] & el Consejo de Europa. (2018). *Handbook on European data protection law*. Agencia de los Derechos Fundamentales de la Unión Europea. http://doi.org/10.2811/343461

Antevenio. (13 de marzo de 2019). *Qué es el web scrapping y para qué sirve*. https://www.antevenio.com/blog/2019/03/que-es-el-web-scraping-y-para-que-sirve/

Almunia, J. (26 de noviembre de 2012). *Competition and personal data protection*. Comisión Europea. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_860

Autorité de la Concurrence & Bundeskartellamt. (10 de mayo de 2016). *Competition Law and Data*. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2

Australian Competition & Consumer Commision. (2 de septiembre de 2017). *Consumer data right (CDR) Project overview*. https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0/cdr-rules-banking

Balagueró, T. (13 de noviembre de 2018). *¿Qué son los datasets y los dataframes en el Big Data?* Deusto Formación. https://www.deustoformacion.com/blog/programacion-diseno-web/que-son-datasets-dataframes-big-data

Banco Central de Reserva del Perú [BCRP]. (mayo 2021). *Reporte de Estabilidad Financiera*. https://www.bcrp.gob.pe/docs/Publicaciones/Reporte-Estabilidad-Financiera/2021/mayo/ref-mayo-2021-recuadro-6.pdf

Banda, L. (2017). *Enforcing Data Portability in the Context of EU*

Competition Law and the GDPR [Tesis de maestría]. MIPLC Master Thesis Series (2016/17). https://ssrn.com/abstract=3203289

Banterle, F. (2019). Data ownership in the data economy: a European dilemma *EU Internet Law in the digital era*, pp. 199-225. https://link.springer.com/chapter/10.1007/978-3-030-25579-4_9

Barker, A. (26 de febrero de 2020). *'Cookie apocalypse' forces profound changes in online advertising*. Financial Times. https://www.ft.com/content/169079b2-3ba1-11ea-b84f-a62c46f39bc2

Bear, Bill. (11 de agosto de 2020). *The tech antitrust hearings are over: What's next for enforcement?* https://www.brookings.edu/blog/techtank/2020/08/11/the-tech-antitrust-hearings-are-over-whats-next-for-enforcement/

Begoña, O. (2013). *El debate sobre la interoperabilidad informática en el derecho de autor comunitario*. [Tesis de doctorado, Universidad de Santiago de Compostela]. Minerva Repositorio Institucional DA USC (Universidad de Santiago de Compostela). https://minerva.usc.es/xmlui/handle/10347/10620

Bolaños, G. (5 de febrero de 2021). *Jurídica: Las cookies en sitios web*. El Peruano. https://elperuano.pe/noticia/114743-juridica-las-cookies-en-sitios-web

Bourne, R. (18 de junio de 2019). *Is This Time Different? Schumpeter, the Tech Giants, and Monopoly Fatalism*. CATO Institute. https://www.cato.org/publications/policy-analysis/time-different-schumpeter-tech-giants-monopoly-fatalism

Büchner, T. (2010). *Die rechtlichen Grundlagen der Übertragung virtualler Güter*. Nomos.

Brandeis, L. & Warren, S. (1890). The right to privacy. *Harvard law review*, *4*(5),193-220. https://www.stetson.edu/law/studyabroad/spain/media/Wk3.Stuart.Day1-1-THE-RIGHT-TO-PRIVACY-(excerpt).pdf

Brown, I. (30 de Julio de 2020). Interoperability as a tool for competition regulation. https://doi.org/10.31228/osf.io/fbvxd

Cadwalladr, C. and E. Graham-Harrison (17 de marzo de 2018). *Revealed: 50 million*

Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Cámara Peruana de Comercio Electrónico [CAPECE]. (2021). *Reporte Oficial de la Industria Ecommerce en Perú* (ed. 2021). https://www.capece.org.pe/wp-content/uploads/2021/03/Observatorio-Ecommerce-Peru-2020-2021.pdf

Cárdenas Krenz, R. (2020). ¿Tienen derechos los muertos? *Giuristi: Revista De Derecho Corporativo*, *1*(1), 171-197. https://doi.org/10.46631/Giuristi.2020.v1n1.09

Castro, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *IUS ET VERITAS*, *18*(37), 260-276. https://www2.congreso.gob.pe/sicr/biblioteca/Biblio_con.nsf/999a45849237d86c052577920082c0c3/2D674102C83D89680525811C00709C7F/$FILE/IUS37P260.PDF

Ciani, J. (2018). A Competition-Law-Oriented Look at the Application of Data Protection and IP Law to the Internet of Things: Towards a Wider 'Holistic Approach'. *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, 216-243. https://doi.org/10.1007/978-3-662-57646-5_9

Ciuriak, D. (2018). *Rethinking Industrial Policy for the Data-driven Economy*. CGI Papers, (192). https://www.cigionline.org/publications/rethinking-industrial-policy-data-driven-economy/

Comisión Europea. (2020a). *DOCUMENTO DE TRABAJO DE LOS SERVICIOS DE LA COMISIÓN que acompaña al documento […] COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO. La protección de datos como pilar del empoderamiento de los ciudadanos y el planteamiento de la UE de cara a la transición digital: dos años de aplicación del Reglamento General de Protección de Datos*. [COM(2020) 264 final]. https://op.europa.eu/es/publication-detail/-/publication/86218ff5-de14-11ea-adf7-01aa75ed71a1/language-es/format-PDF/source-217382351

EUR-LEX. Access to European Union law. (s/f). *Glossary*. https://eur-lex.europa.eu/eli-register/glossary.html

Crémer, J., de Montjoye, Y.A. & Schweitzer, H. (2019). *Competition policy for the digital era*. Comisión Europea. https://doi.org/10.2763/407537

Cress, M. (10 de junio de 2019). *The Black Box Problem.* Artificial Intelligence Mania. http://artificialintelligencemania.com/2019/01/10/the-black-box-problem/

Ctrl-Shift. (2018). *Data mobility: The personal data portability growth opportunity for the UK economy*. UK Department for Digital, Culture, Media & Sport. https://www.ctrl-shift.co.uk/reports/DCMS_Ctrl-Shift_Data_mobility_report_full.pdf

Dalla Corte, L. (2018). Information Technology and Law Series. En: B. Van Loenen, G. Vancauwenberghe, & J. Crompvoets (Eds.). *The European right to data protection in relation to open data*, 30, 127-148. https://doi.org/10.1007/978-94-6265-261-3_7

Davies, J. (30 de abril de 2020). *Why is Google so interested in Fitbit?* Telecoms.com. https://telecoms.com/504015/why-is-google-so-interested-in-fitbit/

Diez Canseco Núñez, L. (2012). Teoría del cuello de botella: las facilidades esenciales. *THEMIS Revista De Derecho*, (61), 65-93. http://revistas.pucp.edu.pe/index.php/themis/article/view/9033

Canal EDteam. (4 de abril de 2019). *¿Qué son las APIs y para qué sirven?* [Archivo de Vídeo]. Youtube. https://www.youtube.com/watch?v=u2Ms34GE14U

Eguiguren, F. (2004a). El nuevo Código Procesal Constitucional peruano. *Derecho PUCP (Revista de la Facultad de Derecho PUCP)*, (57), 161-183. https://doi.org/10.18800/derechopucp.200401.009

Eguiguren, F. (2004b). *La libertad de expresión e información y el derecho a la intimidad personal – Su desarrollo actual y conflictos*. Palestra.

Eguiguren, F. (2015). El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú. *Themis*, 131-140.

El País. (21 de septiembre de 2021). *Medios de toda América llamamos a defender el valor del periodismo profesional en el ecosistema digital*. AMI (Asociación Colombiana de Medios de Información). https://ami.org.co/medios-de-toda-america-llamamos-a-defender-el-valor-del-periodismo-profesional-en-el-ecosistema-digital/

Engels S. & Bernd J. (2018). The Portability Regulation (Regulation (EU) 2017/1128):

A Commentary on the Scope and Application. *JIPITEC (Journal of Intellectual Property, Information Technology and E-Commerce Law)*, 179-200. https://www.jipitec.eu/issues/jipitec-9-2-2018/4728/JIPITEC_9_2_2018_179_Engels_Nordemann

Facebook Inc. (22 de octubre 2020). *Condiciones del servicio.* Facebook. https://www.facebook.com/legal/terms

Exposito-Rosso, Cao, Piquet, Medjaoui (s.f.). *Research Report GDPR Data Portability: The Forgotten Right.* ALIAS. https://cellar-c2.services.clever-cloud.com/alias-code-is-law-assets/static/report/gdpr_data_portability_the_forgotten_right_report_full.pdf

Frické, Martin. (2019). Knowledge pyramid. The DIKW hierarchy. *ISKO Encyclopedia of Knowledge.* http://www.isko.org/cyclo/dikw

Facebook (2021). *Descargar tu información*. https://www.facebook.com/dyi/?referrer=yfi_settings

Graef, I., Husovec, M. & Purtova, N. (2018). Data Portability and Data Control: Lessons for an Emerging Concept in EU Law. *German Law Journal*, *19*(6), 1359-1398. cambridge.org/core/services/aop-cambridge-core/content/view/5904FB88DDC1B9E6EC651A7F89058433/S2071832200023075a.pdf/data-portability-and-data-control-lessons-for-an-emerging-concept-in-eu-law.pdf

Graef, I., Tombal, T. & de Streel, A. ().2019 *Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law*. TILEC Discussion paper DP 2019-024. http://dx.doi.org/10.2139/ssrn.3494212

Graef I., Wahyuningtyas S. & Valcke P. (2015). Assessing data access issues in online platforms, *Telecommunications Policy*, *39*(5), 375-387. http://dx.doi.org/10.1016/j.telpol.2014.12.001

Granville, K. (19 de marzo de 2018). *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens.* The New York Times. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Gómez-Barroso, J. L., y Feijóo-González, C. (2013). Información Personal: La Nueva

Moneda de la Economía Digital. *El profesional de la información*, *22*(4), 290-297. http://oa.upm.es/id/eprint/25807/contents

Google (s.f.). *Ayuda del Cuenta de Google*. https://support.google.com/accounts/answer/3024190#zippy=%2Cexportaciones-programadas

Herrero C. (2006). *Los contratos vinculados (tying agreements) en el derecho de la competencia*. La Ley.

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [INDECOPI]. (2013). Análisis de las funciones del Indecopi a la luz de las decisiones de sus órganos resolutivos, Libre competencia. https://repositorio.indecopi.gob.pe/bitstream/handle/11724/5564/libre_competencia.pdf?sequence=1&isAllowed=y

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [NDECOPI]. (2020a). *Guía Práctica para la protección mediante Secretos Empresariales*. https://bit.ly/3iqRl7n

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [INDECOPI]. (2020b). *Guía de Programas de Cumplimiento de las normas de Libre Competencia*. INDECOPI. https://www.indecopi.gob.pe/documents/51771/4663202/Gu%C3%ADa+de+Programas+de+Cumplimiento+de+las+Normas+de+Libre+Competencia/

International Organization for Standardization & International Electrotechnical Commission. (2018). *ISO/IEC 19944:2017. Information technology — Cloud computing — Cloud services and devices: Data flow, data categories and data use [Tecnología de la información - Computación en la nube - Servicios y dispositivos en la nube: flujo de datos, categorías de datos y uso de datos]*. https://www.iso.org/standard/66674.html

International Organization for Standardization & International Electrotechnical Commission. (2014). *ISO / IEC 17788: 2014(en). Tecnología de la información - Computación en la nube - Descripción general y vocabulario.* https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

International Organization for Standardization & International Electrotechnical

Commission. (2014). *ISO/IEC 25000:2014 Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (Square) — Guide to Square [Ingeniería de Sistemas y Software - Requisitos y Evaluación de Calidad de Sistemas y Software (Cuadrado) - Guía De Cuadrado]*. https://www.iso.org/standard/64764.html

Janeček, V. (2018). Ownership of Personal Data in the Internet of Things. *Computer Law & Security Review*, *34*(5), 1039-1052. http://dx.doi.org/10.2139/ssrn.3111047

Janssen, H., Cobbe, J., Norval, C., & Singh, J. (2020). Decentralised Data Processing: Personal Data Stores and the GDPR, *10*, *356–384*. https://dx.doi.org/10.2139/ssrn.3570895

Open Data Charter [ODC]. (2015). *International Open Data Charter*. https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter_F.pdf

Kitchin R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE Publications.

Kresalja Rosselló, B., & Quintana Sánchez, E. (2005). La doctrina de las facilidades esenciales y su recepción en el Perú. *IUS ET VERITAS*, *15*(31), 59-89. http://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/12409

Lasserre, B., & Mundt, A. (2017). Competition Law and Big Data: The Enforcers' View. *Antitrust & Public Policies*, *4*(1). http://dx.doi.org/10.12870/iar-12607

Li, W. (2018). *A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation*. International Data Privacy Law.

López, R. (9 de octubre de 2019). *Big Data en la Economía Digital*. Forbes. *https://forbes.es/empresas/53509/big-data-en-la-economia-digital/*

León, L. (2011). Manipulación de Información Personal y Derechos Fundamentales. Crítica del proyecto de "ley de protección de datos personales". *Actualidad Jurídica*. (pp.1-10). https://www.academia.edu/713133/Manipulación_de_información_personal_y_derechos_fundamentales_Cr%C3%ADtica_del_proyecto_de_ley_de_protección_de_datos_personales_

León, L. (2006). *Derechos de la personalidad y medios de comunicación* [Tesis de

doctorado, Scuola S. Anna di Pisa]. https://www.academia.edu/713128/Leysser_Le%C3%B3n_Derechos_de_la_personalidad_y_medios_de_comunicaci%C3%B3n_Tesis_de_doctorado_2006_

Lynskey, O. (2019). Grappling with "data power": normative nudges from data protection and privacy. *Theoretical Inquiries in Law*. *20*(1), 189-220. https://doi.org/10.1515/til-2019-0007

Marr, B. (5 de marzo de 2018). *Here's Why Data Is Not The New Oil*. Forbes. https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#18f869a63aa9

Mayer-Schönberger, V. & Cukier, K. (2014). *Big data: a revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt Publishing Company.

Mayer-Schönberger, V., & Padova, Y. (2016). Regime Change? Enabling Big Data through Europe's New Data Protection Regulation. *Science and Technology Law Review*, *17*(2). https://doi.org/10.7916/stlr.v17i2.4007

Masconteiner. (27 de agosto de 2020). *Economía de escala y economía de alcance: ¿son lo mismo?* MasContainer. https://www.mascontainer.com/economia-de-escala-y-economia-de-alcance-son-lo-mismo/

McNamee R. (2019). *Zucked: Waking Up to the Facebook Catastrophe*. Penguien Press.

Mcleod J. (7 de febrero de 2020). *Inside the kill zone: Big Tech makes life miserable for some startups, but others embrace its power*. Financial Post. https://financialpost.com/technology/inside-the-kill-zone-big-tech-makes-life-miserable-for-some-startups-but-others-embrace-its-power

Muñoz, P. J. (2016). El «prosumidor» como figura clave en el desarrollo del derecho del consumo derivado del mercado digital. *Revista CESCO de Derecho de Consumo,* (19), 41-51. https://revista.uclm.es/index.php/cesco/article/view/1127

Nieves 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), 195–239. https://doi.org/10.5944/rdp.85.2012.10723

Novero G. (5 de marzo de 2021) *Google limitará cookies de terceros: ¿qué significa?* Agencia de Publicidad en México.

https://www.grupoendor.com/google-cookies-de-terceros/

Hardinges, K., & Whitworth G. (15 de febrero de 2020). *Will GDPR and data portability support innovation?* Open Data Institute [ODI]. https://theodi.org/article/will-gdpr-and-data-portability-support-innovation/

Open Knowledge Foundation (s.f.). *Open Data Handbook Glossary, Structured Data*. http://opendatahandbook.org/glossary/en/terms/structured-data/

Ostven, M. & Irion, K. (2018). The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?. *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?,* 8-25. https://doi.org/10.1007/978-3-662-57646-5_2

Organización para la Cooperación y el Desarrollo Económico [OECD]. (2008). *Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information*. https://legalinstruments.oecd.org/public/doc/122/122.en.pdf

Organización para la Cooperación y el Desarrollo Económico [OECD]. (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers*, 220. https://doi.org/10.1787/5k486qtxldmq-en

Organización para la Cooperación y el Desarrollo Económico. (2019a). *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*. OECD Publishing. https://doi.org/10.1787/276aaca8-en

Organización para la Cooperación y el Desarrollo Económico. (2019b). *OECD Business and Finance Outlook 2019: Strengthening Trust in Business*. *OECD Publishing*. https://doi.org/10.1787/af784794-en

Organización para la Cooperación y el Desarrollo Económico. (2015). *Data-Driven Innovation: Big Data for Growth and Well-Being.* OECD Publishing http://dx.doi.org/10.1787/9789264229358-en

Plataforma digital única del Estado peruano. (7 de abril de 2021). El Indecopi presenta propuesta normativa para regular el comercio electrónico en el Perú. https://www.gob.pe/institucion/indecopi/noticias/396888-el-indecopi-presenta-propuesta-normativa-para-regular-el-comercio-electronico-en-el-peru

Peukert, A. (2011). Sonstige Gegenstände“ im Rechtsverkehr. En S. Leible, M.

Lehmann, & H. Zech, *Unkörperliche Güter* (pp. 95-122). Tübingen: Mohr Siebeck.

Productivity Commission. (31 de marzo de 2017). *Productivity Commission Inquiry Report: Data Availability and Use*. Australian Government. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology* (pp. 40-81).

Australian Government. Productivity Commission. (2017). *Data Availability and Productivity Commission Inquiry Report, 87*. https://www.pc.gov.au/inquiries/completed/data-access/report/data-access.pdf

Rankin, J. (18 de mayo de 2017). *Facebook fined £94m for 'misleading' EU over WhatsApp takeover*. The Guardian. https://www.theguardian.com/business/2017/may/18/facebook-fined-eu-whatsapp-european-commission

Real Academia de la Lengua Española [RAE]. (2021). *Diccionario de la Lengua Española. Actualización 2020.* https://dle.rae.es/portar?m=form

Red Iberoamericana de Protección de Datos [RIPD]. (10 de junio de 2017). *Estándares de protección de datos para los países Iberoamericanos.* https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

Red Hat. (s.f.). *Diferencias entre Rest y Soap.* https://www.redhat.com/es/topics/integration/whats-the-difference-between-soap-rest

Red Hat. (s.f.). *¿Qué és una API? Qué son las API y para qué sirven.* https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

Ritter, J. & Mayer, A. (2017). *Regulating data as property: a new construct for moving forward*. Duke L. & Tech. Rev., *16*, (220-276).

Rauhofer, J. & Lynskey, O. (2019). *Review of Commonwealth model laws on data protection.* Edinburgh: University of Edinburgh School of Law. 2-17.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*, *33*(2), 163–180.

https://doi.org/10.1177/0165551506070706

Saldaña, M. N. (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), 195-239. https://doi.org/10.5944/rdp.85.2012.10723

United Nations Conference on Trade and Development [UNCTAD]. (2019). *Problemas de competencia en la economía digital. Conferencia de las Naciones Unidas sobre Comercio y Desarrollo*. https://unctad.org/meetings/en/SessionalDocuments/ciclpd54_en.pdf

Plataforma digital única del Estado peruano. (s.f.). Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros [SGTD] https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital

Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros [SGTD]. (29 de julio de 2021). *Documento de Trabajo del Diseño de la Estrategia Nacional de Gobierno de Datos (2021-2026).* https://cdn.www.gob.pe/uploads/document/file/2050181/Dise%C3%B1o%20de%20la%20Estrategia%20Nacional%20de%20Gobierno%20de%20Datos.pdf

Scassa, T. (2018). Data Ownership. *Centre for International Governance Innovation – CIGI Papers*, (187).

Schumpeter, J. (2006). *Capitalism, Socialism and Democracy*. Routledge (ed. 6).

Schneier, B. (2010). *A Taxonomy of Social Networking Data. IEEE Security & Privacy Magazine, 8*(4), 88–88. https://doi.org/10.1109/msp.2010.118

Stapp, A. (8 de octubre de 2019). *Why Data Is Not The New Oil*. Truth on the market. https://truthonthemarket.com/2019/10/08/why-data-is-not-the-new-oil/#:~:text=2.,use%20by%20non-authorized%20parties.&text=This%20contrasts%20with%20oil%2C%20where%20complete%20excludability%20is%20the%20norm.

Superintendencia de Banca, Seguros y AFP [SBS]. (diciembre 2018). Pagos digitales: tomando un nuevo impulso. *Boletín Semanal SBS Informa*. (38). https://www.sbs.gob.pe/boletin/detalleboletin/idbulletin/1132?title=Pagos%20digitales:%20tomando%20un%20nuevo%20impulso

Techopedia. (s.f.). *Granular Data What Does Granular Data Mean?*

https://www.techopedia.com/definition/31722/granular-data

Tovar, T. (2009). La doctrina de las facilidades esenciales: ¿derecho de la competencia o regulación económica? *Advocatus*, (020), 345-361. https://doi.org/10.26439/advocatus2009.n020.3045

Tyco Integrated Fire & Security. (8 de abril de 2014). *¿En qué consiste exactamente un sistema de cámaras CCTV?* Johnson Controls Blog. https://blogseguridad.tyco.es/productos/que-es-sistema-camaras-cctv/

Twitter (2021). *How to download your Twitter archive*. https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive

Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of things. *Personal and Ubiquitous Computing*, *22*(2), 317-332.

Ursic, H. The Failure of Control Rights in the Big Data Era: Does a Holistic Approach Offer a Solution?. En Bakhoum, M.; Conde, B., Mackenrodt, M-O., Surblytė-Namavičienė, G. (2018). *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?* (pp.56-79). MPI Studies on Intellectual Property and Competition Law. https://doi.org/10.1007/978-3-662-57646-5_2

Wilson, C. (2019). *Sleepy Hollow and the Arrovian Legend: Is There a Generalizable Relationship Between Concentration and Innovation.* Federal Trade Commission of United States of America. https://www.ftc.gov/system/files/documents/public_statements/1544375/wilson_concurrences_nyc_remarks_9-12-19.pdf

Wong, J., & Henderson, T. (2018). How Portable is Portable? Exercising the GDPR's Right to Data Portability. En *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive andUbiquitous Computing and Wearable Computers* (911-920).

Wong, J., & Henderson, T. (2019). The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law*, *9*(3), 173-191. https://doi.org/10.1093/idpl/ipz008

Ximénez de Sandoval, P. (30 de junio de 2016). *Alvin Toffler, visionario de la economía*

del conocimiento. El País. https://elpais.com/elpais/2017/09/20/alterconsumismo/1505913507_555679.html

Yakowitz J (2011). Tragedy of the data commons. *Harvard Journal of Law & Technology*, *25*,1.

Zech, H. (2016). Data as a Tradeable Commodity. In A. De Franceschi (Ed.), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution* (pp. 51-80). Intersentia. https://doi.org/10.1017/9781780685212.004

Zingales, L. & Rolnik, G. (30 de junio de 2017). *A way to own your social-media data*. The New York Times. https://www.nytimes.com/2017/06/30/opinion/social-data-google-facebook-europe.html?_r=1

Normativa

Carta de los Derechos Fundamentales de la Unión Europea. (7 de diciembre de 2000). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12016P/TXT&from=DE

Civil Code. Division 3, Part 4, Title 1.81.5. California Consumer Privacy Act [CCPA] 2018, Art. 1798-100. (28 de junio de 2018). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) Secretaría. 2019. Cuestiones de competencia en la economía digital. *Conferencia de las Naciones Unidas sobre Comercio y Desarrollo* (10-12 Julio de 2019). https://unctad.org/system/files/official-document/ciclpd54_es.pdf

Comisión Europea. (19 de febrero de 2020b). Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una estrategia europea de datos. COM (2020) 66. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

Comisión Europea, Comunicación de la Comisión Orientaciones sobre las prioridades de

control de la Comisión en su aplicación del artículo 82° del Tratado CE a la conducta excluyente abusiva de las empresas dominantes. (24 de febrero de 2009) C 45/02.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009XC0224%2801%29#ntr49-C_2009045EN.01000701-E0049

Constitución Política del Perú. (30 de diciembre de 1993).
http://spijlibre.minjus.gob.pe/normativa_libre/main.asp

Decreto Legislativo Nº 1412, Decreto legislativo que aprueba la Ley de Gobierno Digital. (13 de setiembre de 2018).
https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf

Decreto Supremo Nº 003-2013/MINJUS. (22 de marzo de 2013).
http://spijlibre.minjus.gob.pe/normativa_libre/main.asp

Directiva (UE) 2019/944 del Parlamento Europeo y del Consejo sobre normas comunes para el mercado interior de la electricidad y por la que se modifica la Directiva 2012/27/UE (5 de junio de 2019).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32019L0944

Grupo de trabajo del Artículo 29 [GT 136]. (20 de junio de 2007). Dictamen 4/2007 sobre el concepto de datos personales.
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Grupo de trabajo sobre protección de datos del Artículo 29 [GT 242 rev.01]. (5 de abril de 2017). Directrices sobre el derecho a la portabilidad de los datos.
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Grupo de trabajo sobre protección de datos del Artículo 29 [GT 259 rev.01]. (10 de abril de 2018). Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679.
https://ec.europa.eu/newsroom/article29/items/623051/en

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [LGPDPPSO]. (26 de enero de 2017).
http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo119547.pdf

Ley Nº 29733, Ley de Protección de Datos Personales. (03 de julio de 2011).
http://spijlibre.minjus.gob.pe/normativa_libre/main.asp

Ley Nº 28237, Código Procesal Constitucional. (31 de mayo de 2004). http://spijlibre.minjus.gob.pe/normativa_libre/main.asp

Parlamento Europeo y del Consejo, Reglamento UE 2016/679. (27 de abril de 2016). Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. http://data.europa.eu/eli/reg/2016/679/oj

Parlamento Europeo y del Consejo, Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo. (25 de noviembre de 2015). Sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) no 1093/2010 y se deroga la Directiva 2007/64/CE. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015L2366

Proyecto de Ley N° 7870/2020-PE, Ley que crea la Autoridad Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. (10 de junio de 2021). https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL07870-20210610.pdf

Proyecto de Ley N° 2986/20, "Proyecto de Ley sobre Protección de Datos Personales" (12 de diciembre de 2020). https://www.senado.gob.ar/parlamentario/comisiones/verExp/2986.20/S/PL

Resolución SBS Nº 504-202, Aprueban el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, modifican el Reglamento de Auditoría Interna, el Reglamento de Auditoría Externa, el TUPA de la SBS, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, el Reglamento de Riesgo Operacional, el Reglamento de Tarjetas de Crédito y Débito y el Reglamento de Operaciones con Dinero Electrónico. (19 de febrero de 2021). https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-para-la-gestion-de-la-seguridad-de-la-resolucion-no-504-2021-1929393-1/

Resolución Directoral Nº 019-2013-JUS/DGPDP. (11 de octubre de 2013). http://spijlibre.minjus.gob.pe/normativa_libre/main.asp

Resolución de Consejo Directivo Nº 286-2018-CD-OSIPTEL, Texto Único Ordenado del Reglamento de Portabilidad Numérica en el Servicio Público Móvil y el Servicio de Telefonía. (25 de septiembre de 2020).

Secretaría de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo [UNCTAD]. (2020). Examen voluntario entre homólogos del derecho y la política de protección del consumidor del Perú. https://unctad.org/system/files/official-document/ditccplp2020d1_es.pdf

Jurisprudencia

BverfG [Tribunal Constitucional Federal], Urteil [Sentencia] des Ersten Senats [Primer Senado]. (15 de diciembre de 1983). 1 BvR 209/83 -, Rn. 1-215. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

Curia Europea. CONCLUSIONES DEL ABOGADO GENERAL SR. ANTONIO TIZZAN O. CONCLUSIONES DEL SR. TIZZANO — ASUNTO C-418/01 (2 de octubre de 2003). https://curia.europa.eu/juris/showPdf.jsf;jsessionid=51B247696D406C6BF3863FBC3B97CC7B?text=&docid=48679&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=22434766

Dirección General de Protección de Datos Personales. Expediente Nº 042-2017-PTT, Resolución Directoral Nº35-2019-JUS/DGPDP. (8 de mayo de 2015). https://cdn.www.gob.pe/uploads/document/file/604164/RD-35-2019-DGTAIPD.pdf

Dirección de Protección de Datos Personales. Opinión Consultiva Nº 34-2020-JUS/DGTAIPD. (14 de julio de 2020) https://cdn.www.gob.pe/uploads/document/file/1745107/Sobre%20solicitud%20de%20acceso%20a%20los%20datos%20personales%20y%20acceso%20a%20la%20informaci%C3%B3n%20p%C3%BAblica.pdf.

Dirección General de Protección de Datos Personales. Expediente Nº 013-2015-PTT, Resolución Directoral Nº 044-2015-JUS/DGPDP. (31 de diciembre de 2015). https://cdn.www.gob.pe/uploads/document/file/582293/RD-044-2015-DGPDP.pdf

Dirección de Protección de Datos Personales. Expediente Nº 004-2017-PTT, Resolución Directoral Nº 378-2017-JUS/DGTAIPD- DPDP. (1 de septiembre de 2017). https://cdn.www.gob.pe/uploads/document/file/589686/RD-378-2017-DPDP.pdf

Dirección de Protección de Datos Personales. Expediente Nº 005-2019-PTT, Resolución

Directoral N° 1220-2019-JUS/DGTAIPD-DPDP. (16 de mayo de 2019). https://cdn.www.gob.pe/uploads/document/file/606239/RD-1220-2019-DPDP.pdf

Dirección de Protección de Datos Personales. Expediente Nº 050-2017-PTT, Resolución Directoral N° 1427-2018-JUS/DGTAIPD-DPDP. (26 de junio de 2018). https://cdn.www.gob.pe/uploads/document/file/605080/RD-1427-2018-DPDP.pdf

People-Browsr, Inc. et al v. Twitter Inc. (People-Browsr), N°C-12-6120 EMC (N.D. Cal. Mar. 6, 2013).

Tribunal General (Sala Cuarta). Sentencia al Asunto T - 79/12. Cisco Systems, Inc. y Messagenet SpA contra Comisión Europea. (11 de diciembre de 2013. ECLI:EU:T:2013:635). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62012TJ0079

Tribunal Constitucional. Sala Primera. Expediente N° 1797-2002-HD/TC, Lima, Wilo Rodríguez Gutiérrez. (29 de enero de 2003). https://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

Tribunal Constitucional. Sala Primera. Expediente Nº 04739-2007-PHD/TC, Lima, Pesquera Virgen Del Valle S.A.C. (15 de octubre de 2007). http://www.justiciaytransparencia.pe/sentencias/datos_expediente/desarrollo.php?SECTION_ID=275&ELEMENT_ID=927&SEARCH_R=/sentencias/datos_expediente/resultados.php?arrFilter_ff%5BNAME%5D=4739

Tribunal Constitucional. Sala Primera. Expediente Nº 00693-2012-PHD/TC, Lambayeque, José Manuel Curipuma Alburqueque. (24 de julio de 2012). https://www.tc.gob.pe/jurisprudencia/2013/00693-2012-HD.html

Tribunal Constitucional. Expediente Nº 06164-2007-HD/TC, Arequipa, Jhonny Robert Colmenares Jiménez. (21 de diciembre de 2007). http://justiciaytransparencia.pe/sentencias/des_buscador.php?ULTIMA_SECCION=252&SECCION_ID=252&ELEMENT_ID=774&BUSQUEDA=6164&ETIQUETAS=

Anexo