El dato personal como insumo productivo en la actividad empresarial y su protección jurídica[1]

Personal data as productive input in business activity and its legal protection

María Cristina Quintero Riveros[2]

RESUMEN

No son novedosas aquellas inquietudes que han surgido con relación al uso y aprovechamiento que realizan las empresas de los datos de sus usuarios y consumidores. Mayoritariamente la regulación se ha desarrollado desde una perspectiva constitucional, orientada a la protección a los derechos fundamentales de los originadores de los datos. Esta situación parece desconocer de manera alguna la importancia que estos datos tienen de cara a la estructuración de un modelo de negocio. Por tal motivo, este trabajo estudia de una parte los tipos y naturaleza de los datos que pueden recolectarse y usarse para fines empresariales, e igualmente su importancia para los empresarios. De otro lado, se analiza la coherencia del tratamiento jurídico que se da a los datos en función de su naturaleza y uso, así como se persigue establecer si desde el derecho privado se pueden proteger los datos personales como insumo de la actividad empresarial.

Para el desarrollo de este trabajo se utilizó una metodología de investigación socio jurídica con un énfasis principalmente cualitativo, concretado en el análisis de fuentes legales, jurisprudenciales y doctrinarias, así como la elaboración de estudios de campo.

1 Fecha de recepción: 14 de octubre de 2023 Fecha de Aceptación: 14 de noviembre de 2023.
DOI:https://doi.org/10.18601/16923960.v22n2.10

2 Abogada de la Universidad Externado de Colombia y Magister en Derecho Comercial de la misma casa de estudios. Correo: maria.quintero06@est.uexternado.edu.co

A partir de esta investigación se identificaron dinámicas de mercantilización del dato personal, que hacen visible la necesidad de asignarles un tratamiento jurídico *ius privatista* al uso y aprovechamiento de estos por parte del empresario. Asimismo, se distinguió el ámbito de protección de las normas de protección de datos vigentes y las situaciones que escapan a dicha órbita, siendo merecedoras de un tratamiento jurídico acorde con la realidad empresarial. Estos hallazgos permitieron visibilizar esta circunstancia y enfatizar en la necesidad de observar los fenómenos económicos y sociales presentes en los distintos estamentos de la sociedad, a fin de valorar la necesidad, efectividad y coherencia de la regulación vigente.

Palabras clave: Datos personales, bases de datos, propiedad intelectual, mercantilización, metadatos, insumo, activo, secreto empresarial.

ABSTRACT

The concerns that have arisen regarding the use and exploitation that companies make of the data of their users and consumers are not new. For the most part, regulation has been developed from a constitutional perspective, aimed at protecting the fundamental rights of data originators. This situation seems to in no way ignore the importance that this data has when it comes to structuring a business model. For this reason, this work studies, on the one hand, the types and nature of data that can be collected and used for business purposes, and also its importance for entrepreneurs. On the other hand, the coherence of the legal treatment given to the data is analyzed based on its nature and use, as well as the aim is to establish whether personal data can be protected from private law as an input to business activity.

To develop this work, a socio-legal research methodology was used with a mainly qualitative emphasis, specified in the analysis of legal, jurisprudential and doctrinal sources, as well as the preparation of field studies.

From this research, dynamics of commercialization of personal data were identified, which make visible the need to assign a private ius legal treatment to the use and exploitation of these by the businessman. Likewise, the scope of protection of the current data protection regulations and the situations that escape said orbit were distinguished, being worthy of legal treatment in accordance with business reality. These findings made this circumstance visible and emphasized the need to observe the economic and social phenomena present in the different levels of society, to assess the need, effectiveness, and coherence of the current regulation.

Keywords: Personal data, databases, intellectual property, commercialization, metadata, input, asset, business secret.

INTRODUCCIÓN

¿Qué es el dato? ¿Qué tipos de datos existen? ¿Qué datos se generan en los entornos digitales? ¿Cómo hace uso las empresas de nuestros datos? ¿Es legítimo que las empresas usen nuestros datos? ¿Qué normas disciplinan dicho aprovechamiento de los datos personales? Estas, y varias más, son las inquietudes que surgen a la hora de examinar las dinámicas actuales de la economía digital.

En la actualidad los mercados digitales ocupan gran parte de la vida de los individuos y, en consecuencia, se han vuelto un objeto de estudio importante para el Derecho, desde múltiples perspectivas. Una parte importante de los aspectos que ha buscado estudiar el Derecho es la privacidad en entornos digitales, de ahí que con regularidad sea noticia sanciones en contra de las grandes empresas por el uso de los datos de los consumidores.

No obstante, señala el Foro Económico Mundial[3] que los datos son el nuevo petróleo, Empresas como Uber, Rappi, Google, Amazon, entre miles otras, hacen uso de los datos de sus consumidores o usuarios y es en ese aprovechamiento que se cimienta su modelo de negocio. Algunos sugieren que los datos son un activo empresarial, un insumo o que incluso podría asimilarse a otro factor de producción. Dada esa importancia que reviste el dato personal para el empresario, un cuestionamiento legítimo que surge es si existe algún mecanismo a través del cual pueda proteger ese elemento necesario para el desarrollo de su actividad.

En atención a lo anterior, el presente escrito pretende abordar de manera interdisciplinar esta problemática. Para el efecto, se estudiará la literatura técnica, gerencial y jurídica pertinente para entender qué es un dato personal, los tipos de datos presentes en entornos digitales, su aprovechamiento por parte de las empresas y el régimen jurídico vigente. A partir de ello, el análisis versará sobre la determinación de cuál categoría jurídica permite proteger el interés que el empresario tiene sobre estos datos, entendiendo que estos últimos son parte fundamental de su negocio.

Así, los objetivos de esta investigación son, en primera instancia, comprender la perspectiva del empresario, el interés que tiene sobre los datos, los usos que les da y la forma en que esto beneficia al negocio. Como segundo propósito está ahondar en los conceptos técnicos asociados con los datos recolectados en entornos digitales, con el fin de comprender la vigencia de esta discusión y por qué antes en el curso de la humanidad no surgieron tantas inquietudes a propósito de la privacidad como ahora. En tercer lugar,

3 Foro Económico Mundial, & Bain & Company Inc. Personal data : The emergence of a new asset class. (2011). https://www3.weforum.org/docs/WEF _ ITTC _PersonalData-NewAsset_Report_2011.pdf

se busca tener un panorama más claro de la regulación a propósito de la protección de datos, pretendiendo establecer la intención del regulador frente al uso de datos personales.

Todos estos objetivos secundan la resolución de la pregunta de investigación, a saber, ¿Puede el empresario proteger los datos personales que fungen como insumo de su actividad? Para brindar respuesta a dicho cuestionamiento, a continuación se presenta la revisión de la literatura relevante para la materia.

1. REVISIÓN DE LITERATURA

A efectos de la elaboración del presente escrito se revisó y analizó literatura doctrinal de cara a establecer el estado actual del escenario gerencial y jurídico sobre el aprovechamiento de los datos personales por las empresas.

Para comenzar, se revisaron textos de carácter doctrinal en materia de computación de datos y semántica, a efectos de determinar el significado del *dato*. Teniendo claro este concepto, se realizó un análisis de las definiciones legales de datos personales, en contraste con definiciones encontradas en textos doctrinales y estudios elaborados por entidades no gubernamentales. Lo anterior como quiera que estos recursos permitieran establecer si existe o no claridad sobre el concepto de datos personales.

De otra parte, se estudió desde la perspectiva técnica y gerencial la relevancia de los datos y el Big Data en la actividad empresarial, especialmente sus usos y la forma en que esto beneficia la productividad de la organización. Con todo lo anterior, la revisión de literatura finalizó por brindar un panorama de las disposiciones en materia de protección de datos personales, con atención a la óptica gerencial explicada con anterioridad.

1.1. ¿QUÉ ES EL DATO?

Sobre la noción de datos, se evidencia que en los textos jurídico-normativos este concepto se reduce a información. Entre las fuentes que aluden a esta noción se encuentran las siguientes: En el orden jurídico nacional, el literal c) del artículo 3º de la Ley 1581 de 2012 indica que Dato Personal es *"Cualquier información…"*[4]. De otra parte, en el Derecho Europeo el artículo 4º del Reglamento 2016/679 de 27 de abril de 2016 del Parlamento Europeo define al Dato Personal como *"toda información…"*[5].

4 Congreso de la República de Colombia. [Ley 1581 de 2012]. Por la cual se dictan disposiciones generales para la protección de datos personales. (2012).

5 Parlamento Europeo. Reglamento 2016/679: Reglamento General de Protección de Datos,(2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

En consonancia con lo anterior, desde la semántica la Real Academia de la Lengua Española define al Dato como *"Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho"*. Las definiciones expuestas son similares y permiten concluir que la noción de *dato* es estrictamente relacional, pues se estructura en función de la información y de otro tipo de factores.

Desde la metodología científica o la ciencia de datos se ha estudiado el dato de manera más extensa, pero igualmente desde una perspectiva relacional, en conjunto con nociones como las de "conocimiento" e "información". Pese a lo anterior, no se brindan definiciones precisas sobre el vocablo *"datos"*. Autores como Briones Delegado citando a Fritz Machlup lo relaciona intrínsecamente con la información, estableciendo lo siguiente:

> *"En palabras de Machlup, la información es "un flujo de mensajes o significados que pueden añadir, reestructurar o cambiar el conocimiento". **Son los datos a los cuales se les ha asignado significado por medio de una conexión relacional**. Se trata de las materias primas que constituyen el punto de partida del conocimiento, de las que se ha dicho que pueden existir en cualquier forma (utilizable o no) y que no tienen un significado por sí mismas".* (Negrilla fuera del texto original)[6]

La definición recogida por Briones Delgado se acompasa con las definiciones legales y semánticas expuestas. No dista mucho la aproximación hecha desde otras disciplinas tales como la epistemología, donde autores como Birger Hjørland[7], quien también entiende la noción del dato de manera relacional con el concepto de información, indica más precisamente que el dato constituye el sustrato principal para llegar a la información y posteriormente al conocimiento. En ese sentido, Hjørland considera que la información es, en esencia, datos entendidos y procesados, mientras que el conocimiento se configura a partir de la interpretación de la información.

Dicha postura también se encuentra respaldada en la literatura jurídica, aunque con algunas precisiones importantes. Janeček sostiene que los datos pueden dar lugar a información, dependiendo de la forma en que aquellos sean interpretados, por lo que se aprecia que, si bien son nociones relacionadas, se trata de conceptos diferentes[8]. Así, a su juicio la regulación tiene un punto de partida erróneo al equiparar la información con el dato. Luego,

6 Jesús Mariano Briones Delgado, Datos, información y conocimiento: promesas y realidades de la red global (Madrid: Universidad Complutense de Madrid, 2014)

7 Berjer Hjørland, "Data (With Big Data and Database Semantics)", Official Journal of the International Society for Knowledge Organization 45, n. º 8 (2018), pp. 685-708

8 Vlacav Janeček, "Ownership of personal data in the Internet of Things", Computer Law and Security 34, n. º 5 (2018). https://doi.org/10.1016/j.clsr.2018.04.007

para Janeček resulta esencial distinguirlos de cara a establecer si es posible que exista un derecho de propiedad sobre los datos.

En el campo de la formulación de política pública la situación no es muy diversa. El CONPES No. 3920 de 2018 acoge una definición de carácter etimológico, concluyendo que los datos son la representación de variables cualitativas y cuantitativas[9]. Ahora, si bien esta definición no está, en principio, formulada desde una perspectiva relacional; lo cierto es que posteriormente indica que tras el proceso de recolección, almacenamiento y procesamiento surge información como sustrato de producción de conocimiento.

Las nociones expuestas dan cuenta principalmente de dos situaciones relevantes de cara al estudio que se pretende realizar. En un primer término, las definiciones expuestas conllevan a la necesidad de deslindar el concepto de datos de los *datos personales*, de cara a brindarles un tratamiento jurídico especial a estos últimos. A los efectos de la presente investigación se abordarán especialmente los datos personales, al ser una categoría jurídica merecedora de una protección especial, por lo que se procederá a revisar su concepto desde la perspectiva normativa, de política pública y académica.

1.2. Los datos personales

Las definiciones legales de datos personales no distan mucho entre sí. De esta forma, con el fin de evidenciar la homogeneidad en su definición y, por ende, en su tratamiento jurídico, se hará alusión a la definición contemplada en el ordenamiento jurídico colombiano, en contraste con las disposiciones que se encuentran en otras jurisdicciones.

El literal c) del artículo 3 de la Ley 1581 de 2012 señala que los datos personales son: *"Cualquier información* ***vinculada o que pueda asociarse*** *a una o varias* ***personas naturales determinadas o determinables***" (Negrilla fuera del texto original). De manera análoga, el artículo 2 de la Ley 25.326 de la República Argentina define los datos personales, así: *"Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"*. El literal v) del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares de México, establece igualmente que los datos personales son: *"cualquier información concerniente a una persona física identificada o identificable"*.

Como se aprecia, las definiciones de *datos personales* aquí relacionadas guardan coherencia con las definiciones semánticas de *datos*, aunque no

9 Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación. Documento CONPES 3920. (2018).

con las precisiones hechas por Hjørland[10] y Janeček[11] respecto del elemento diferencial entre datos e información. Asimismo, las definiciones referidas dan cuenta de que el concepto de datos personales conlleva un elemento transcendental que determina la existencia de un tratamiento jurídico diferencial, esto es, la identificabilidad del sujeto. No obstante, ninguna de las definiciones aludidas precisa cuándo o de qué manera se entiende que una persona es identificable a través de un dato.

De otra parte, el numeral del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados mexicana profundizó el concepto de datos personales, detallando el componente de identificabilidad, como también se advierte en la legislación comunitaria europea. Veamos: *"Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información".*[12]

En consonancia, el numeral 1 del artículo 4 del Reglamento General de Protección de Datos de la Unión Europea (RGPD en adelante) dispone de manera más precisa que el dato personal es:

> *"toda* ***información 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"* (Negrilla fuera del texto original)[13].

Como se aprecia en las definiciones recopiladas, la más completa y omnicomprensiva es la contenida en el RGPD. Adicionalmente, califica que se podrán considerar datos personales aquellos que permitan identificar a una persona de manera directa o indirecta, siendo este un punto crucial en lo que refiere a los datos personales en entornos digitales.

Desde la orilla de la política púbica, en Colombia el documento CONPES No. 3920 del Consejo Nacional de Política Económica y Social ha definido al dato personal como aquel que permite la individualización de un sujeto,como

10 Berjer Hjørland, "Data (With Big Data and Database Semantics)", Official Journal of the International Society for Knowledge Organization 45, n. º 8 (2018), pp. 685-708

11 Vlacav Janeček, "Ownership of personal data in the Internet of Things", Computer Law and Security 34, n. º 5 (2018). https://doi.org/10.1016/j.clsr.2018.04.007

12 Congreso General de los Estados Unidos Mexicanos. Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados 2017. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

13 Parlamento Europeo. Reglamento 2016/679. Reglamento General de Protección de Datos de la Unión Europea. (2016). https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

por ejemplo su nombre, edad, estatura, etc.; mientras que el dato impersonal es aquel que, o bien se refiere a un fenómeno ajeno a una persona (ej. Temperatura, cantidad de transeúntes, etc), o no permite la identificación de un sujeto en concreto.[14]

De acuerdo con el mismo documento, la importancia de esta clasificación radica en el nivel de publicidad o apertura que podrán tener dichos datos[15]. Dicha definición se encuentra respaldada también por otros organismos supranacionales como el Consejo de Europa, que mediante el Convenio 108+ para la protección de las personas con relación al procesamiento de datos personales, el cual establece en el artículo 2º que el dato personal *es "aquella información a un sujeto identificado o identificable"*[16].

A continuación, se revisarán algunas clasificaciones de los datos, haciendo especial énfasis en los datos personales. Posteriormente, se hará hincapié en los datos recolectados en los entornos digitales, en lo que se incluye el comercio electrónico, redes sociales, aplicaciones para dispositivos móviles, entre otros.

1.3. ¿Qué tipos de datos personales existen?

Normativamente en el ordenamiento jurídico colombiano la Ley 1266 de 2008, Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013 prevén otras categorías sucedáneas a los datos personales. Estas son el **dato público privado**, el **dato sensible** y el **dato semiprivado**. Veamos algunas de estas definiciones:

El primero de estos es definido por vía negativa y de ejemplificación por el literal f) del artículo 3 de la Ley 1266 de 2009, así:

> *"Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas".*[17]

14 Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación, (2018)

15 Ibíd.

16 Consejo de Europa. Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos trasfronterizos de datos. (2018). https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

17 Congreso de la República de Colombia. [Ley 1266 de 2008]. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de

Ahora bien, a efectos de decantar este concepto el Decreto Reglamentario 1377 de 2013 amplió esta definición al invocar que:

> *"Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva"*[18].

Aunado a lo anterior, la Registraduría Nacional del Estado Civil (en adelante la Registraduría) ha señalado que el dato público privado *"Es aquel que puede ser consultado por cualquier persona,* ***sin autorización del titular****. Entre estos se encuentra el número de identificación, apellidos, lugar y fecha de expedición del documento de identidad"* (Negrilla fuera del texto original)[19]

En relación con el dato sensible, si bien la Ley 1581 de 2012 refiere aspectos sobre su tratamiento, no la define. Empero, el numeral 3 del artículo 3 del Decreto Reglamentario 1377 de 2013 los define como aquellos que:

> *"afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos".*[20]

Igualmente, buscando decantar esta noción, la Registraduría ha brindado su concepto al señalar que estos se relacionan con la intimidad del titular y que puedan revelar el origen racial, étnico, orientación política, convicciones religiosas o filosóficas, entre los que se incluyen también datos de salud, biométricos y de orientación sexual[21].

servicios y la proveniente de terceros países y se dictan otras disposiciones. (2008). DO: [47.219].

18 Presidencia de la República de Colombia. [Decreto Reglamentario 1377, 2013]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. (2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

19 Registraduría Nacional del Estado Civil. Grupo de acceso a la información y protección de datos personales. (2023). https://registraduria.gov.co/IMG/pdf/Folleto_web.pdf

20 Presidencia de la República de Colombia. [Decreto Reglamentario 1377, 2013]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015. (2013). https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

21 Registraduría Nacional del Estado Civil. Grupo de acceso a la información y protección de datos personales. (2023). https://registraduria.gov.co/IMG/pdf/Folleto_web.pdf

Por último, los datos personales privados con respecto al dato financiero son definidos por el literal g) del artículo 3 de la Ley 1266 de 2008, así:

> *"Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley".*[22]

Ahora, pese a que la Ley 1581 de 2012 ni el Decreto Reglamentario 1377 de 2013 no define los datos personales privados, ni refiere a su tratamiento, la Registraduría ha aterrizado esta noción al indicar que: *"Es aquel dato que, además de ser de interés para el titular, puede generar interés para cierto sector u otro grupo de personas. Incluye dentro de tal clasificación información tal como la fecha y lugar de nacimiento"*[23]

Ahora bien, tal y como se señala en la sentencia C-748 de 2011[24], estas categorías establecidas por el legislador son arbitrarias y, por consiguiente, no son las únicas formas de clasificar los datos personales, más aún si se considera el advenimiento de las nuevas tecnologías y la digitalización, que permiten la captura de nuevos tipos de datos y generar así nuevas clasificaciones.

En línea con lo anterior, procedamos a revisar los tipos de datos personales que se incluyen en las legislaciones argentina, mexicana y el ordenamiento jurídico-comunitario europeo, con el fin de establecer similitudes y diferencias en las clasificaciones legales de los datos y la vigencia de tales clasificaciones de cara a las dinámicas tecnológicas y de mercado actuales.

Comenzando por lo dispuesto en la Ley 25.326 de la República Argentina, allí se incluyen como categorías especiales de los datos personales a los datos sensibles y los datos relativos a la salud. Los primeros son definidos por el artículo 2 de la mencionada Ley de manera muy similar a lo contemplado en la legislación colombiana, indicando que son aquellos que *"revelan origen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual"*[25]. En cuanto a

22 Congreso de la República de Colombia. [Ley 1266 de 2008]. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (2008). DO: [47.219].

23 Registraduría Nacional del Estado Civil. Grupo de acceso a la información y protección de datos personales. (2023). https://registraduria.gov.co/IMG/pdf/Folleto_web.pdf

24 Corte Constitucional. Sentencia C-748 de 2011. Control de constitucionalidad al Proyecto de Ley Estatutaria No. 184 de 2010 Senado; 046 de 2010 Cámara, "por la cual se dictan disposiciones generales para la protección de datos personales" Magistrado Ponente: Jorge Ignacio Pretelt Chaljub (2011)

25 Honorable Congreso de la Nación Argentina. [Ley 25326/2000]. Ley de Protección de los Datos Personales. (2000). https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

la segunda categoría, estos no son definidos, pero de manera muy general y respecto de su tratamiento, el artículo 10 del mismo estatuto señala que son aquellos relativos a la salud física o mental de los pacientes.

En relación con la legislación mexicana el escenario no es diverso. El numeral 6 del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares incluye la categoría de datos sensibles, definiéndolos en un sentido similar a las ya expuestas, agregando algunos componentes subjetivos tales como *"la afectación a la esfera más íntima de su titular o conlleve un riesgo grave para este"*.[26]

Para referirnos a la legislación comunitaria europea, debe hacerse alusión en primer término al RGPD, cuyos numerales 13, 14 y 15 del artículo 4 incluyen las categorías de datos genéticos[27], biométricos[28] y relativos a la salud[29]. Como se aprecia, el legislador europeo no consideró una clasificación como la que se evidenció antes, pero precisamente profundiza en conceptos más concretos, sin que ello afecte el espectro de protección, como quiera que la definición de datos personales es amplia y omnicomprensiva, como ya se señaló.

Sin perjuicio de lo anterior, la Directiva 2002/58 CE del Parlamento Europeo y Consejo de Europa, en relación con la privacidad y las comunicaciones electrónicas introduce los conceptos de **dato de tráfico y dato de localización**. El literal b) del artículo 2 de éste define los primeros como *"cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"*[30]. En relación con los segundos, el literal c) de la misma norma, indica que se trata de *"cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público"*[31].

26 Congreso General de los Estados Unidos Mexicanos. Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados 2017. https://www.diputados.gob.mx/LeyesBiblio/pdf/lgpdppso.pdf

27 Estos son entendidos como: *"datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona"*.

28 datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos

29 datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud

30 Diario Oficial de las Comunidades Europeas. Directiva 2002/58/CE del parlamento europeo y del consejo. (2002). https://www.boe.es/doue/2002/201/L00037-00047.pdf

31 Ibíd.

Aun cuando las propias definiciones no refieren a estos últimos como datos personales en estricto sentido, conviene precisar que la Directiva establece una estructura de tratamiento especial al considerar que en este tipo de datos y comunicaciones puede existir información íntima de los sujetos que deba ser protegida conforme al Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales[32].

Desde la orilla de la política pública, en Colombia la Dirección Nacional de Planeación en el documento CONPES No. 3920 de 2018 expone diversas clasificaciones de dato. Entre ellas se encuentra una primera clasificación que, destaca el documento, tiene repercusiones sobre el tratamiento jurídico del mismo.[33]. De acuerdo con este documento, pueden existir datos públicos o privados y personales o impersonales, atendiendo los primeros a un criterio orgánico que responde al sujeto que origina el dato y los segundos a las variables que representa el dato.

Es preciso destacar que el mencionado documento expone la política pública colombiana en materia de Big Data y su explotación, por lo que no se limita a referirse a los datos desde la perspectiva analógica. De ahí entonces que este documento nos precise qué tipos de datos se pueden considerar como digitales, indicando que se trata de aquellos que son interpretados mediante codificación binaria y señando que *"Estos últimos pueden generarse de dos maneras: por la interacción de personas con sistemas, herramientas y servicios digitales o automáticamente por programas de software y dispositivos de hardware que los capturan"*.[34]

Continuando con dicha línea discursiva, propone otra clasificación de datos en función de la organización y almacenamiento de datos digitales, en la que identifica que existen datos no estructurados, semi estructurados y estructurados. Agrega además que, a partir del análisis de estos en conjunto con otros, surge un nuevo concepto al que denomina *datos enlazados*. Estos últimos, los define como métodos para la visualización, intercambio y/o conexión de datos en internet.[35].

Esta noción de datos enlazados lleva a hablar de otros conceptos que han surgido académica y jurisprudencialmente alrededor de los datos personales, como lo es la categoría de *dato personal compuesto* a la que hace alusión Polo Roca[36], con ocasión de la decisión *Digital Rights Ireland y otros* (asuntos

32 Ibíd.

33 Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación. Documento CONPES 3920. (2018).

34 Consejo Nacional de Política Económica y Social, Departamento Nacional de Planeación. Documento CONPES 3920. (2018).

35 Ibíd.

36 Andoni Polo Roca. Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos. University of Deusto. (2021). pp. 211-240

C-293/12 y C-594/12). En la mencionada decisión se analizan otros datos como los obtenidos a partir de los datos de comunicaciones, advirtiéndose que, si bien hay datos que en un principio pueden considerarse como no personales, de ser analizados en conjunto con otros datos relacionados pueden brindar datos de una persona identificable[37].

Para la OCDE, citando a Schneier, los datos personales también pueden sub-clasificarse de la siguiente manera:

> i) *"Datos de servicio: entendidos como aquellos otorgados para la apertura de una cuenta.*
>
> ii) *Datos divulgados: entendidos como aquellos que el usuario voluntariamente entrega.*
>
> iii) *Datos confiados: siendo estos, por ejemplo, aquellos comentarios que los usuarios de internet hacen en publicaciones ajenas.*
>
> iv) *Datos incidentales: siendo datos relativos a un usuario en específico, pero cargados por otra persona.*
>
> v) *Datos de comportamiento: aquellos que contienen información de las acciones de los usuarios en uso de sitios web.*
>
> vi) *Datos deducidos: entendidos como aquella información que puede deducirse de los datos divulgados por otra persona"*[38].

Con posterioridad el mismo organismo indica algunos ejemplos de lo que considera datos personales. Mediante el reporte "Exploring the economics of personal data: A survey for measuring monetary value" enlista los siguientes como datos personales:

> *"i) Contenidos generados por los usuarios, como blogs y comentarios, fotos y vídeos, etc.*
>
> *ii) Datos de actividad o comportamiento, incluyendo lo que la gente busca y mira en Internet, lo que la gente compra en línea, cuánto y cómo paga, etc.*
>
> *iii) Datos sociales, incluidos los contactos y amigos en las redes sociales,*

37 Tribunal de Justicia de la Unión Europea. Digital rights Ireland Ltd & Seitlinger y otros. (2014). https://eur-lex.europa.eu/legal-content/es/txt/pdf/?uri=celex:62012CJ0293&from=es

38 Organización para la Cooperación y el Desarrollo Económicos. (OCDE). Exploring the Economics of Personal Data: A survey of methodologies for measuring monetary value. (2013). https://doi.org/https://doi.org/10.1787/5k486qtxldmq-en https://www.oecd-ilibrary.org/content/paper/5k486qtxldmq-en

iv) Datos de localización, incluidas las direcciones residenciales, el GPS y la geolocalización (por ejemplo, de los teléfonos móviles), la dirección IP, etc.

teléfonos móviles), dirección IP, etc.

v) Datos demográficos, incluidos la edad, el sexo, la raza, los ingresos, las preferencias sexuales, la afiliación política, etc.

vi) Datos identificativos de carácter oficial, incluidos el nombre, la información financiera y los números de cuenta, la información sanitaria, los números de la seguridad social o de la sanidad nacional, los antecedentes policiales, etc.".[39]

Por contera, desde la doctrina Janeček[40] estima que la línea divisoria entre el concepto de datos personales y no personales es ambigua y dinámica, como quiera que los distintos ordenamientos jurídicos delimitan más o menos restrictivamente esta noción. Señala el autor que tal circunstancia se hace patente al revisar las posturas de la justicia comunitaria europea en contraste con, por ejemplo, la jurisprudencia del Tribunal Federal de Australia[41]. Con esto en mente, estima que debería distinguirse o clasificarse entre información intrínsecamente personal e información extrínseca. Para tal efecto señala que, de acuerdo con la Corte Europea de Derechos Humanos en los asuntos *Aycaguer v. Francia*[42] y *S. y Marper v. Reino Unido*[43], se hace referencia al carácter intrínsecamente privado de la información genética de una persona. Partiendo de tal afirmación y de cara a establecer la posibilidad de que exista un derecho de propiedad sobre los datos, habrá de excluirse de tal análisis los datos intrínsecamente personales, como quiera que:

"(…) estos datos son constitutivos de la propia identidad, porque "no hay diferencia entre la esfera informativa [interpretada por estos datos intrínsecamente personales] y la identidad personal. (…) Por lo tanto, la propiedad de estos datos implicaría conceptualmente la propiedad

39 Ibíd. p. 8

40 Vlacav Janeček, "Ownership of personal data in the Internet of Things", Computer Law and Security 34, n. º 5 (2018). https://doi.org/10.1016/j.clsr.2018.04.007

41 Desde la perspectiva europea, a partir de las normas de derecho positivo es bastante claro que información como los metadatos (concepto que se explicará in extenso en el siguiente apartado) pueden ser considerados como personales, a partir del concepto de identificabilidad indirecta al que refiere el numeral 1 del artículo 4 del RGPD, pues se apela a un concepto amplio de identificabilidad. En contraposición, al revisar la sentencia dictada por el Tribunal Federal de Australia en el asunto Privacy Comissioner v. Telstra Corporation Limited se evidencia que allí se somete a examen la expresión "relativa a una persona" con el fin de determinar su alcance y si los metadatos pueden ser considerados como un dato personal bajo esa óptica.

42 Corte Europea de Derechos Humanos. Sección Quinta. Aplicación 8806/12.

43 Corte Europea de Derechos Humanos. Sala General. Aplicaciones 30562/04 y 30566/04.

de la identidad de las personas y el propietario de los datos intrínsecamente personales sería el propietario de la identidad de las personas".

Pese a la complejidad de las afirmaciones de Janeček, resulta valioso reconocer estas clasificaciones de datos personales de cara a establecer el tratamiento jurídico apropiado para cada una de estas categorías jurídicas. De esa manera, es viable cuestionarse sí la amplitud en el concepto de identificabilidad supone -o no- un obstáculo en la capacidad identificar qué tipos de datos personales habrán de tener un tratamiento jurídico más riguroso, en atención a la protección del legítimo interés del empresario de proteger tales datos como insumo de su actividad.

Con fundamento en lo anterior, se profundizará brevemente en los tipos de datos captados en los entornos digitales y algunas técnicas de rastreo con notable incidencia en la problemática propuesta. Posteriormente, se estudiará la literatura relativa al aprovechamiento que hacen las empresas de estos, la forma en que se genera valor a través de su procesamiento y la importancia que estos tienen para el empresario.

1.4. El internet y los datos

Al margen de las clasificaciones de datos que proponen los textos legislativos, se puede advertir la existencia de otros tipos de información que cobran especial relevancia cuando de mercados digitales se trata, pues como lo menciona González Guerrero: *"Cada interacción con la tecnología deja un rastro susceptible de ser recolectado, almacenado, analizado y correlacionado con otros datos"*[44].

Bajo ese entendido, autores como González Guerrero exponen que los datos generados a partir del uso de internet pueden ser identificados mediante tecnologías de rastreo (TR en adelante). Para Sánchez-Rola *et al.*[45] las TR o *Web Tracking Techniques* permiten la recolección de datos de los usuarios de internet, tales como los historiales y configuraciones de búsqueda en internet, con el fin de ser usados para distintas actividades comerciales y no comerciales en la web. Tal situación la respalda González Guerrero al indicar que: *"las tecnologías de rastreo (tr) producen récords de las páginas web que se visitan, los clics en las páginas, las búsquedas en internet, las interacciones en redes sociales, las compras en línea y la ubicación de las personas"*[46].

44 Laura Daniela González Guerrero. «Control De Nuestros Datos Personales En La Era Del Big Data: El Caso Del Rastreo Web De Terceros». *Estudios Socio-Jurídicos* 21(1). 2019. https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941.

45 Iskander Sánchez Rola, et al. The web is watching you: A comprehensive review of web-tracking techniques and countermeasures. *Logic Journal of the IGPL*, *25*(1), (2017). pp. 18-29.

46 Laura Daniela González Guerrero. «Control De Nuestros Datos Personales En La Era

Con fundamento en lo anterior, afirma González Guerrero que las *cookies* son una especie de técnicas de rastreo, que permiten recolectar información de navegación del usuario. Ante lo anterior, cabe cuestionarse qué tipo de información se obtiene a través de estas. En respuesta a dicho interrogante, Kristol[47] indica que las *cookies* son: *"(…) la pieza de información que el servidor y el cliente intercambian en doble vía. La cantidad de información es usualmente pequeña y su contenido es a discreción del servidor"*. Tal concepto es acogido por Google, quienes mediante su sitio web de ayuda han brindado la siguiente definición:

> *"Las cookies son archivos que crean los sitios web que visitas. Guardan los datos de navegación para mejorar la experiencia online. Gracias a ellas, los sitios web pueden mantener la sesión abierta, recuerdan tus preferencias y te proporcionan contenido basado en tu ubicación"*[48]

En punto al tipo de información que puede ser captado mediante las *cookies*, advierte González Guerrero que:

> *"Por ejemplo, almacenan la información de inicio de sesión de tal forma que, en un nuevo acceso, no es necesario proporcionar usuarios y contraseñas. Al comprar en internet y elegir un producto, esta información se almacena en una cookie a la que el servidor tiene acceso para recordar las selecciones. Las cookies también pueden registrar las secciones que una persona visita en un sitio web, lo que permite medir el contenido más popular, el menos visitado y cómo llegan, usualmente, las personas al portal. Esta información sirve para mejorar el rendimiento de los portales"*[49].

Varios de estos usos también son reconocidos por Kristol, aunque haciendo una precisión importante, en tanto que la información que podrá ser recolectada mediante las *cookies* dependerá, en gran medida, de la información que el usuario explícitamente entregue. Si bien lo anterior es cierto, debe también considerarse que las interacciones entre el ser humano y los dispositivos generan datos, sobre los cuales el usuario no es completamente consciente, también denominados por algunos autores como datos pasivos. Veamos:

> *"Una vea que conectas un sistema a una red abierta, los datos que produce y los que producimos nosotros al llevarlo en el bolsillo se multiplican y van más allá de las páginas web visitadas,*

Del Big Data: El Caso Del Rastreo Web De Terceros». *Estudios Socio-Jurídicos* 21 (1). 2018. https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941.

47 David Kristol. HTTP Cookies: Standards, privacy, and politics. ACM Transactions on Internet Technology (TOIT), 1(2), (2001). pp. 151-198.

48 Google. Página de ayuda de Google Chrome. (2022). https://support.google.com/chrome/answer/95647?co=genie.Platform%3DDesktop&hl=es#:~:text=Las%20cookies%20son%20archivos%20que,contenido%20relevante%20seg%C3%BAn%20tu%20ubicaci%C3%B3n

49 Laura Daniela González Guerrero. «Control De Nuestros Datos Personales En La Era Del Big Data: El Caso Del Rastreo Web De Terceros». Estudios Socio-Jurídicos 21 (1). 2019. p. 214. https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941.

> *los anunciados clicados -aunque sea por error- o las palabras tecleadas. Todas las máquinas que intervienen en el proceso (nuestro PC , los routers, los servidores de contenidos y comunicaciones, las antenas de comunicaciones…), todos ellos, sin excepción, generan datos pasivos"*[50]

En consecuencia, la afirmación de Kristol[51] puede encontrar contradictores. Como lo menciona Llaneza, en los entornos digitales se recolectan grandes cantidades de datos pasivos, por lo que muchas veces los usuarios desconocen la información que están produciendo mediante la utilización de un dispositivo electrónico y, por ende, no son absolutamente conscientes de los datos que se están entregando.

En términos generales, hay quienes afirman que los datos son un subproducto de la informática y, en esa medida, muchos de los datos generados en entornos digitales serán pasivos[52].

Existen innumerable cantidad de ejemplos de ello, a modo de guisa encontramos los teléfonos celulares, relojes de actividad o los dispositivos inteligentes para el hogar, pues todos estos captan datos que posteriormente son usados con distintas finalidades. Para autores como Scheier[53] estos datos derivados de la interacción entre humanos y computadores es denominada como *metadatos*. Este último concepto no ha contado con una definición diáfana, pues como bien señala Bargmeyer *et al.*, se han entendido como datos sobre otros datos. Ante tal ambigüedad, estos autores indican que los metadatos *"son datos usados para describir otros datos"*[54], mientras para Schneier se trata de *"la información que usa un sistema de computación para operar o los datos que es un subproducto de dicha operación"*.[55]

Pese a la inespecificidad del término, lo cierto es que los dispositivos de uso recurrente generan incontables cantidades de metadatos que serán almacenados y, probablemente, tratados y analizados en conjunto con otra información. Entonces, serán metadatos los datos generados por las aplicaciones que usamos, los reportes de uso o actividad de nuestros dispositivos móviles, entre muchos otros derivados de la interacción que voluntaria o involuntariamente sostenemos con todos los dispositivos computarizados que rodean nuestra cotidianidad.

50 Paloma Llaneza González. Datanomics: todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos. (Editorial Planeta, 2019). p.25.

51 David Kristol. HTTP Cookies: Standards, privacy, and politics. ACM Transactions on Internet Technology (TOIT), 1(2), (2001). pp. 151-198.

52 Bruce Schneier. Data and Goliath : the hidden battles to collect your data and control your world. (2018).

53 Ibíd.

54 Bruce Bargmeyer, et al. Metadata standards and Metadata registries: an overview. (Vasa. 2000).

55 Bruce Schneier. Data and Goliath : the hidden battles to collect your data and control your world. (2018).

Como se aprecia, las interacciones que tenemos con nuestros dispositivos de computación generan un creciente volumen de datos, que deben ser agregados en masa y en corto tiempo, para ser aprovechables por las empresas intensivas en uso de datos, bien para perseguir la eficiencia en algunas actividades propias de la empresa o para crear nuevas líneas de negocio. Claramente, tal producción, recolección, agregación y tratamiento de datos en masa ha suscitado más de una inquietud respecto de la protección de datos personales. Para comprender esas preocupaciones, a continuación se estudiará brevemente la noción del *Big Data* y las discusiones que ha suscitado en punto a la protección de datos.

1.5. La agregación masiva de datos, el Big Data, el Internet de las Cosas (IoT) y el aprovechamiento de estos por parte del empresariado

Como se expuso en los apartados anteriores, el aumento en los sistemas de computación y gracias a la forma en que estos se han integrado a la cotidianidad de cada persona, la producción de datos es cada vez mayor. Derivado de tal generación de datos e información, han surgido conceptos como el Big Data y el internet de las cosas, los cuales han generado nuevas oportunidades de negocio y, a su vez, cuestionamientos a propósito del tratamiento de datos personales. Dado lo anterior, se expondrán brevemente estos conceptos para, posteriormente, entrar a estudiar la forma en que tal producción de datos ha devenido relevante -y en algunos casos hasta indispensable- para los empresarios.

1.5.1. El Big Data

Para la OCDE aún no existen definiciones claras de Big Data[56] y, aunque se trata de un tema ampliamente abordado en el mundo académico, no hay una definición precisa al respecto. En términos generales la mayoría de las definiciones coinciden en resaltar las cuatro principales características del Big Data: i) volumen, ii) velocidad, iii) variedad y iv) valor[57]. Autores como De Mauro *et al*[58] buscaron unificar los distintos criterios usados para definir el Big Data, llegando a establecer la siguiente definición:

56 Organización para la Cooperación y Desarrollo Económicos. (OCDE). Data-Driven Innovation (2015). https://doi.org/https://doi.org/10.1787/9789264229358-en

57 Pfeiffer Castellanos. Digital economy, big data and competition law. (Mkt.& Competition L, 2019). p. 3-53.

58 Andrea De Mauro, et al. What is big data? A consensual definition and a review of key research topics. Paper presented at the *AIP Conference Proceedings, 1644*(1) (2015). pp. 97-104.

> *"Activos de información caracterizados por un volumen, una velocidad y una variedad tan elevados que requieren una tecnología y unos métodos analíticos específicos para su transformación en valor"*[59-60].

Pese a que dichas características son esenciales para comprender el rol de los datos en la economía digital, advierte la OCDE que las definiciones basadas en estas propiedades pueden conllevar a equívocos, pues se hace referencia a la capacidad de procesamiento de datos no estructurados, más no al término en sí mismo.[61].

Con relación a la velocidad se destaca la importancia con la que se generan datos en el entorno digital, como quiera que pueda llegar a constituir una ventaja competitiva para aquellos empresarios que basen sus decisiones gerenciales en los datos[62] (McAfee et al., 2012).

De otra parte, Castellanos Pfeiffer resalta respecto del volumen que este es, a su criterio, una de las características más evidentes del Big Data. Indican autores como Stucke & Grunes que parte de los motivos que contribuyen al aumento de la recolección y tratamiento de datos en masa es la disminución en los costos[63]. También, hay quienes indican que el aumento en el volumen de datos disponibles se debe al *Internet de las cosas* (IoT por su nombre en inglés)[64]. En todo caso, la doctrina coincide en que la cantidad de datos que pueden generarse, captarse y almacenarse hoy en día es bastante grande y, en esa línea, hay quienes destacan que *"Por ejemplo, se estima que Walmart recolecta más de 2,5 petabytes de datos cada hora de las transacciones con sus clientes. Un petabyte es un cuatrillón de bytes"*[65].

En punto a la variedad, se hace patente la versatilidad del Big Data como herramienta para la toma de decisiones empresariales, pues los datos que allí

59 Andrea De Mauro, et al. What is big data? A consensual definition and a review of key research topics. Paper presented at the AIP Conference Proceedings, 1644(1) (2015). p. 9.

60 Traducción propia. El contenido del texto original es el siguiente: *"Information assets characterized by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value" and as an attribute when denoting its peculiar requisites, e.g. "Big Data Technology" or "Big Data Analytical Methods".*

61 Organización para la Cooperación y Desarrollo Económicos. (OCDE). Data-Driven Innovation (2015). https://doi.org/https://doi.org/10.1787/9789264229358-en

62 Andrew McAfee and Erik Brynjolfsson. Big data: the management revolution. *Harvard Business Review, 90*(10), (2012) p. 60-68

63 Maurice Stucke, y Allen Grunes. Part I The Growing Data-Driven Economy, 2 Defining Big Data. Big Data and Competition Policy (Oxford Competition Law ed, (2016)

64 Bernard Marr, B. *Data strategy: cómo beneficiarse de un mundo de Big Data, analytics e internet de las cosas*. (Ecoe Ediciones, 2018).

65 Andrew McAfee and Erik Brynjolfsson. Big data: the management revolution. Harvard Business Review, 90(10), (2012) p. 60-68

pueden identificarse pueden tomar distintas formas, como lo son los mensajes, fotos, señales de GPS, actualizaciones, entre muchas otras[66].

Dadas dichas características, el aspecto más relevante a destacar es que *"Entorno a este concepto (...) giran múltiples tecnologías que contribuyen a organizar, almacenar y sobre todo, analizar en profundidad los datos"*[67].Tal generación de datos y el avance de las tecnologías de la información que permiten su agregación y procesamiento masivo suponen nuevas oportunidades para que las empresas alcancen ventajas competitivas, pues allí se encuentran un sinnúmero de aplicaciones provechosas para el empresariado.

No obstante, han surgido diferentes cuestionamientos entorno a la naturaleza de los datos que se recolectan en los entornos digitales. La variedad de datos originados y recolectados, así como el volumen y velocidad de procesamiento ponen de presente distintas inquietudes entorno a la protección de datos personales, el derecho a la intimidad e, incluso, ponen sobre la mesa la discusión sobre la vigilancia que ejercen las grandes empresas y los Estados sobre los individuos.[68].

Algunas de estas inquietudes son puestas de presente por autores como Schneier y Véliz[69], quienes en sus textos presentan múltiples ejemplos en los que las empresas hacen uso de los datos de usuarios y consumidores. Claramente, la postura presentada por estos autores tiende a generar mayor consciencia sobre el valor de la privacidad. Sin embargo, su planteamiento se mantiene en considerar que la recolección y tratamiento masivo, automático -y hasta oculto- de tales datos supone una actividad vigilancia sobre los particulares riesgosa y posiblemente constitutiva de violaciones a las libertades civiles, además de ser usada por las empresas con el fin de discriminar, a efectos de clasificar usuarios y consumidores para distinguir los mercados de bienes y servicios que se les presentan y la forma en que son ofertados[70]

Consideraciones similares han surgido en torno al Internet de las Cosas, fenómeno que abordaremos a continuación para, posteriormente, adentrarnos en la perspectiva gerencial sobre el uso de datos personales y no personales para la empresa.

66 Ibíd.

67 Javier Puyol Moreno. Una aproximación a Big Data. Revista de Derecho de La Uned (RDUNED), 14. (2014). pp. 471-506. https://doi.org/10.5944/rduned.14.2014.13303

68 Bruce Schneier. Data and Goliath : the hidden battles to collect your data and control your world. (2018).

69 Carissa Véliz. Privacy is Power. Why and How You Should Take Back Control of Your Data. Internacional Data Privacy Law. (3). https://doi.org/10.1093/idpl/ipac007

70 Op. cit. Schneier.

1.5.2. El Internet de las Cosas

El Internet de las Cosas (en adelante IoT por su nombre en inglés) está cada vez más presente en la vida cotidiana. Desde sistemas de iluminación que se encienden de manera automática, pasando por todo tipo de electrodomésticos inteligentes y hasta carros que se auto-conducen; en todos estos dispositivos está presente el IoT. Este ha sido entendido por autores como Haller *et al.* como:

> *"Un mundo en el que los objetos físicos se integran perfectamente en la red de información, y donde los objetos físicos pueden convertirse en participantes activos en los procesos empresariales. Los servicios están disponibles para interactuar con estos "objetos inteligentes" a través de Internet, consultar su estado y cualquier información asociada a ellos, teniendo en cuenta las cuestiones de seguridad y privacidad"*[71].

Como es natural, estos "objetos inteligentes" se alimentan de datos y producen datos. De acuerdo con lo expuesto en el apartado anterior, muchos de estos datos serán metadatos necesarios para el adecuado funcionamiento del dispositivo. En otros casos, el usuario de estos estará entregando datos, probablemente sin tener mayor consciencia de tal circunstancia, como es el caso de los monitores de actividad física o smartwatches. En términos más precisos: *"La mayoría de las aplicaciones IoT no sólo se centran en la supervisión de eventos puntuales, sino también en la extracción de la información recopilada por los objetos IoT"*[72].

Los datos generados por los sensores de estos dispositivos son un alto volumen de información, variada, rápidamente generada a medida de su uso y que puede tener un gran valor para el empresario, es decir, se trata de Big Data que podrá ser analizado y utilizado para reportar grandes beneficios tanto a las empresas como para los usuarios. De un lado, las empresas pueden percibir beneficios tales como i) generar eficiencias en la toma de decisiones gerenciales, ii) mejorar la ejecución de sus prestaciones mercantiles, sin necesidad de contar con un feedback del usuario y iii) desarrollar nuevas líneas de negocio, entre otros. Desde la perspectiva del consumidor, los datos pueden aportar positivamente en i) la rápida y eficaz respuesta de las empresas en la generación de mejoras, actualizaciones o corrección de inconsistencias de los bienes y servicios ofrecidos, ii) el lanzamiento de nuevos productos y servicios, producto del aprovechamiento de los datos y

71 Stephan Haller. The Internet of things in an enterprise context. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5468. (2009). p. 2 https://doi.org/10.1007/978-3-642-00985-3_2

72 Ejaz Ahmed et al. The role of big data analytics in Internet of Things. *Computer Networks*, (2017). p. 1 https://doi.org/10.1016/j.comnet.2017.06.013

la I+D, iii) la optimización de recursos, particularmente de costos y tiempo, en el desarrollo de ciertas actividades que pueden ser realizadas mediante, por ejemplo, dispositivos que utilizan el IoT, entre otros beneficios.

Tal explotación de datos suscita las mismas inquietudes sobre el respeto a la privacidad a las que se hizo referencia previamente, puntualizándose en que muchos de estos datos revelan aspectos profundos de la intimidad de las personas tales como sus gustos, preferencias y estado de salud, generando una vigilancia constante y profunda de parte de los negocios y el gobierno sobre cada uno de los individuos.[73]

Uno de los ejemplos que denota la sensibilidad de la información generada por dispositivos de IoT es aquel de los datos de salud recolectados por los rastreadores de actividad física. Algunos de los problemas que resultan de la explotación de tales datos son: i) la ambigüedad legal existente respecto de esta información una vez es compartida con terceras partes o en caso de que la sociedad recolectora y tratante de la información caiga en escenarios de insolvencia, ii) los inadecuados estándares de encriptación, iii) la vulnerabilidad de los sistemas de almacenamiento en la nube, iv) la multiplicidad y divergencia en la regulación de protección de datos personales y v) la existencia de mercados de datos y *data brokers* donde se considera la información personal como un *commodity* altamente valorado[74].

Pese lo anterior, es claro que no toda la información generada por los dispositivos de IoT indefectiblemente permitirá la identificación de una persona (bien de manera individual o siendo asociado con otro tipo de información). Piénsese en el ejemplo de los dispositivos de "*Smart home*" como bombillos inteligentes, termostatos, dispositivos de seguridad, entre varios otros, los cuales generan una información sobre la preferencia, costumbres y rutinas, pero que podrá ser de distintas personas que cohabitan un mismo inmueble. Es precisamente respecto de estos casos donde el concepto de identificabilidad al que se refiere la regulación de protección de datos personales puede ser evaluada de cara a las necesidades del empresario. Por ello, a continuación se revisará la literatura de la perspectiva gerencial del uso de datos personales y no personales para los fines de la empresa y se analizarán los resultados obtenidos en dos (2) entrevistas hechas a personas que ocupan cargos gerenciales relacionados con el manejo de datos personales de consumidores y trabajadores.

73 Carissa Véliz. Privacy Is Power: Why and How You Should Take Back Control of Your Data. In International Data Privacy Law (Issue 3). (2022). https://doi.org/10.1093/idpl/ipac007

74 Banerjee, Syagnik et al. Wearable devices and healthcare: Data sharing and privacy. *The Information Society* 34.1 (2018). pp. 49-57

1.6. Perspectiva gerencial: El uso de los datos personales y no personales por parte de las empresas. ¿Cómo las empresas aprovechan sus beneficios?

Con independencia del concepto y vicisitudes del dato personal, la realidad es que los datos han devenido un elemento esencial en la gestión empresarial. La doctrina mayoritaria coincide en que los datos brindan grandes beneficios a las empresas e, incluso, estiman que la recolección de datos ha permitido el desarrollo de nuevas líneas de negocio.[75]

En esa vía, Marr destaca que hay tres principales usos que pueden dar las empresas a los datos: i) mejorar la toma de decisiones, ii) hacer a las empresas más eficientes y aumentar su actividad, y iii) puede constituir una fuente de ingresos nueva adyacente al negocio principal[76].

Hoy en día son múltiples los ejemplos que se pueden encontrar de empresas que utilizan los datos para la apertura de nuevos modelos de negocio o para mejorar procesos al interior de la empresa. De manera somera, presentes en el mercado colombiano podemos pensar en empresas intensivas en el uso de datos como Rappi, fintechs como LuloBank, Ualá o Littio, proptechs como Habi o La Haus, por solo nombrar algunas. Lo anterior sin perjuicio de empresas tradicionales que hacen uso de los datos para mejorar sus procesos, como aquellos relacionados al mercadeo y fidelización.

Lo anterior supone que existen infinitas posibilidades en la forma en que los empresarios pueden aprovechar los datos, llegando en algunos casos a ser un insumo fundamental para el desarrollo de la operación. Ello implica que los datos pueden tener un valor dinerario, pero también su valor puede verse representado en externalidades: *"Muchos de los usos de los datos que pueden crear valor directamente, no necesariamente entrañan una transacción de mercado o pueden ser medidos por una, pero el impacto económico y social es directo"*[77].

Una de estas formas de aprovechamiento que resultan nucleares en el desempeño de la actividad empresarial es coadyuvar la toma de decisiones. Marr resalta que tradicionalmente las decisiones empresariales son tomadas por personas con experiencia y experticia en su campo, por lo que, en alguna medida, dichas decisiones responden a una cierta intuición de negocios. No obstante, el mismo autor destaca que *"todo se reduce a tomar decisiones empresariales*

75 Carrie Gates y Peter Matthews. Data is the new currency. Paper presented at the *Proceedings of the 2014 New Security Paradigms Workshop*, (2014). pp. 105-116.

76 Bernard Marr, Data strategy: cómo beneficiarse de un mundo de Big Data, analytics e internet de las cosas. (Ecoe Ediciones, 2018).

77 Organización para la Cooperación y Desarrollo Económicos. (OCDE). Exploring the Economics of Personal Data: A survey of methodologies for measuring monetary value. (2013). p. 9 https://doi.org/https://doi.org/10.1787/5k486qtxldmq-en https://www.oecd-ilibrary.org/content/paper/5k486qtxldmq-en

mejores y más acertadas [y] Los datos ofrecen la perspectiva necesaria para tomar dichas decisiones"[78]. Por lo tanto, parte del correcto aprovechamiento de los datos por parte de las empresas consiste en buscar respuestas a preguntas centrales del negocio mediante estos. Algunas de estas preguntas se refieren a entender mejor a los clientes y al mercado, o incluso los procesos internos de la empresa y a los empleados.

El autor también indica que los datos pueden aumentar la eficiencia de la empresa, pues

> *"(…) las empresas pueden ganar visibilidad en tiempo real de sus operaciones. Esto aumenta la eficiencia al permitir que se controle cada aspecto de la operación industrial y se ajuste para garantizar un rendimiento óptimo. También ayuda a reducir los tiempos de inactividad en el sentido de que, si sabemos exactamente cuándo hay que reemplazar una pieza desgastada, las máquinas se romperán con menos frecuencia"*[79].

Vale resaltar que, el uso de los datos como posibilidad de mejorar los procesos internos no se circunscribe solamente a aquellos negocios con modelo de operación tradicional, pues, por ejemplo, el modelo de negocio de Uber tiene sus bases en el mismo principio, ya que a través de la colaboración masiva Uber puede determinar la demanda y las tarifas, entre otros aspectos del servicio[80].

En concordancia con las afirmaciones de Gates & Matthews, menciona Marr (2018) que, así como los datos pueden contribuir a la mejora de la operación empresarial, también pueden constituir una nueva línea de negocio. Tal situación es, quizás, la que con más frecuencia se resalta a la hora de hablar del Big Data. Es el caso del negocio de la publicidad online de Facebook[81] y Google, o de empresas como FitBit, IBM o EMIS, quienes venden sus datos o analizan datos de terceros y obtienen ganancias por ello.

Dichas apreciaciones son reconocidas por la OCDE, toda vez que reconoce que el uso de la analítica de datos permite obtener información para comprender mejor, por ejemplo, el comportamiento de las personas, o generar sistemas autónomos para la toma de decisiones[82]. Sin embargo, una de las

78 Bernard Marr. *Data strategy: cómo beneficiarse de un mundo de Big Data, analytics e internet de las cosas*. (Ecoe Ediciones, (2018). p. 22

79 Ibíd. p. 26

80 Bernard Marr, B. Data strategy: cómo beneficiarse de un mundo de Big Data, analytics e internet de las cosas. (Ecoe Ediciones, 2018).

81 Sobre este aspecto en concreto indica Marr que: *"Facebook ofrece otro ejemplo sencillo de este proceso en marcha. La red social es gratuita para los usuarios, pero hace ya mucho tiempo que genera ingresos por la publicidad"* (p. 33).

82 Organización para la Cooperación y el Desarrollo Económico. (OCDE). Data-Driven Innovation (2015). https://doi.org/https://doi.org/10.1787/9789264229358-en

preguntas centrales de este asunto es ¿Por qué los datos pueden favorecer la gestión empresarial?

Uno de los factores que permiten hablar de los beneficios de los datos se refiere a la naturaleza de los datos como un bien no rival. Autores como Llaneza González y Stucke (consideran que los datos son recursos que pueden ser usados más de una vez sin que se agoten. En otros términos:

> *"(…) los economistas indican que los datos personales, en algunas ocasiones, son bienes no rivales, en tanto distintas personas pueden usar estos datos para obtener información, sin que con ello se reduzca el valor de los datos para los demás"*[83].

Dicha situación es reconocida por el Fondo Monetario Internacional, organismo que mediante el informe "The Economics and Implications of Data: An Integrated Perspective", indicó que los datos son bienes no rivales, toda vez que su uso no implica su agotamiento[84].

Destaca la doctrina que, otro aspecto que redunda en los beneficios del Big Data, es que hoy en día los costos de la recolección y almacenamiento de datos se han reducido y el avance en las tecnologías de análisis de datos permite obtener un mayor provecho de estos[85].

En función de lo anterior, para el empresariado y la doctrina los datos entrañan un valor y, por tanto, se consideran como un activo o como un tipo de moneda[86]. Un ejemplo claro de tal consideración es la propuesta elevada por RadioShack en el proceso de insolvencia empresarial al que solicitó su admisión en los Estados Unidos de Norteamérica[87], en la que propuso subastar los datos personales de sus consumidores (e-mail y números de teléfonos), junto con otros activos de la empresa, con el fin de satisfacer el interés de los acreedores del concurso[88].

83 Maurice Stucke y Allen Grunes, A. Part I The Growing Data-Driven Economy, 2 Defining Big Data . Big Data and Competition Policy (Oxford Competition Law ed. 2016). p. 1

84 Yan Carrière Swallow y Vikram Haksar The Economics and Implications of Data: An Integrated Perspective. (2019). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

85 Ibíd.

86 Gates, Carrie y Peter Matthews. "Data is the new currency". *Proceedings of the 2014 New Security Paradigms Workshop*. (2014). pp. 105-116.

87 Fuente de la noticia: https://archive.nytimes.com/dealbook.nytimes.com/2015/02/05/radio-shack-files-for-chapter-11-bankrutpcy/

88 https://www.computerworld.com/article/2901691/new-york-threatens-action-if-radioshack-sells-customer-data.html, https://blogs.law.nyu.edu/privacyresearchgroup/2015/03/radioshacks-bankruptcy-and-auctioning-off-customer-data-a-violation-of-privacy-policy/

Pese a la complejidad que representa dicha afirmación desde el punto de vista jurídico, lo cierto es que no se trata de una opinión aislada, ni concentrada en una sola industria o sector económico. A modo de ejemplo, industrias tradicionales como aquellas enfocadas en la extracción de recursos naturales no renovables también estiman relevantes los datos para el desarrollo de su operación: *"La industria del petróleo y el gas tiende a considerar los datos como información que describe el estado de un activo; por el contrario, los líderes en temas de Big Data consideran que los datos son un activo valioso en sí mismo"*[89].

Esta postura de considerar los datos como un activo es coadyuvada por varios autores, indicándose que *"la recolección, estandarización, procesamiento y venta de grandes cantidades de datos se ha vuelto un gran negocio, los datos como un verdadero activo organizacional susceptible de ser comercializado a nivel internacional"*[90].

En la misma línea, consultoras como Baker Mckenzie y KPMG consideran que los datos o bases de datos constituyen un activo del cual saca provecho el empresario, sin desconocer la dificultad en su tratamiento jurídico, pues como se menciona en el informe de la consultora Baker Mckenzie:

> *"Sin embargo, los datos son bastante diferentes en su naturaleza respecto de otros activos, especialmente en lo relativo a*:
>
> i. *Los datos son intangibles y, en consecuencia, es difícil atribuirles un valor;*
>
> ii. *A diferencia de los commodities cuyo valor radica en la escases o la utilidad, los datos son infinitos, no rivales, fáciles de reutilizar y su valor nace de su uso y su valor nace, generalmente, de la difusión y combinación de los mismos;*
>
> iii. *Los datos no son susceptibles de ser protegidos legalmente como los activos de propiedad intelectual"*[91].

1.7. Aproximación práctica al aprovechamiento de los datos por parte de las empresas

Como parte de la revisión de la literatura del presente artículo y con el fin de establecer el estado del arte sobre la materia, se realizaron dos entrevistas a personas que ocupan cargos gerenciales a propósito del manejo y gestión de datos, de cara a conocer desde la perspectiva práctica de los entrevistados la relevancia de los datos en su actividad y modelo de negocio. Pese a que

89 Robert Perrons, y Jesse Jensen. Data as an asset: What the oil and gas sector can learn from other industries about "Big Data". *Energy Policy, 81*, (2015). pp. 117-121.

90 Konstantinos Domdouzis, et al. Data, An Organisational Asset. In K. *Concise Guide to Databases: A Practical Introduction* (2021). pp. 3-21.

91 Von Dietze, y Geddis, Irvine. Data as an Asset. (2019). p. 7

el detalle de las preguntas respondidas y las conclusiones se detalla en los anexos 1 y 2, se hace preciso destacar algunas de las respuestas brindadas por los entrevistados, como quiera que revelan importante información para los propósitos de este escrito.

Así, para contextualizar un poco las siguientes anotaciones, cabe mencionar que la entrevista que yace en el Anexo 1 versa sobre una empresa del sector Fintech, donde los datos recolectados provienen de usuarios y consumidores de este servicio tecnológico para las finanzas, particularmente giros y remesas al exterior. De otro costado, la entrevista relacionada en el Anexo 2 tiene que ver con un cargo asociado al área de recursos humanos de una empresa de banca tradicional, donde se tratan y usan los datos de los trabajadores de la empresa.

Establecido lo anterior, en relación con la entrevista contenida en el Anexo 1 es preciso destacar que existen sectores económicos donde la recolección de datos por parte de las empresas se convierte en un imperativo categórico para poder operar en el mercado. Ejemplo de ello son las empresas del sector financiero o empresas tecnológicas de servicios financieros (Fintech), que tendrán que recolectar datos personales de sus consumidores para dar cumplimiento a regulaciones sobre prevención de lavado de activos y financiación del terrorismo. Durante la entrevista se refirió a ella como *know your customer* (KYC) y consiste esencialmente en solicitar información básica del cliente para identificarlo y corroborar la veracidad de esta, como parte de un proceso de debida diligencia sobre el cliente (*customer due diligence*).

Ahora bien, al margen de lo anterior, el entrevistado manifestó que en el entorno de las Fintech los datos también pueden ser usados para otras finalidades, entre las que destaca: i) asegurar una debida prestación del servicio, especialmente en lo relativo a la seguridad de las transacciones, ii) diseño de productos o funcionalidades y iii) mercadeo y publicidad.

Al respecto refirió que, aunque para las primeras dos funciones son de gran relevancia los datos de sus clientes o consumidores, es cierto que para efectos de alcanzar mayores audiencias tales datos no son suficientes. De esta forma, una forma de obtener datos personales de nuevo público a quién dirigir la publicidad puede ser la compra de bases de datos, aunque es una práctica obsoleta e insuficiente, como quiera que hoy en día es posible contratar la prestación del servicio de mercadeo con grandes empresas como Meta Platforms Inc. o Google, o adquirir el acceso a bases de datos sin tener que acarrear los costos de limpieza de la información, compliance normativo y la desactualización de dicha información.

En punto a la segunda entrevista, por el rol que desempeña la entrevistada en la organización, esta versa sobre la relevancia de los datos en la toma de decisiones gerenciales, particularmente en lo referente al recurso humano. Así, en consonancia con lo dicho por Marr, los datos en este segmento son usados de cara a mejorar la toma de decisiones, procurando basar estas últimas

los datos analizados, más que en la experiencia, intuición o empirismo como podría haberse hecho en el pasado. A su vez, la entrevistada expresó que ello se acompasa con las nuevas tendencias de las ciencias gerenciales del recurso humano o *human resources management*, donde recientemente se ha visto el auge de la *people analytics*, entendida esta última como *"un proceso o método de la gestión de recursos humanos basado en el uso del big data para captar información sobre el desempeño en el trabajo"*[92].

Aunado a lo anterior, destacó que el rol de los datos en la gestión del recurso humano es crucial. Se hace también necesaria la gestión de los datos personales y sensibles de los empleados para dar cumplimiento regulación a la que se encuentra sometida la empresa. Así, un ejemplo al que refiere la entrevistada es el cumplimiento a la Directiva Europea 2006/54/EC relativa a la aplicación del principio de igualdad de oportunidades e igualdad de trato entre hombres y mujeres en asuntos de empleo y ocupación. De otra parte, dicha información permite anticipar tendencias del mercado laboral, entender las dinámicas salariales, ajustar los planes de remuneración, orientar las políticas de atracción y retención de talentos, entre otros.

Por contera, se precisó un aspecto trascendental respecto de la utilidad de los datos. Para la entrevistada, el valor de tales datos no yace en el dato en sí mismo, sino en la limpieza, depuración, procesamiento y análisis que se hace sobre este. Si bien más adelante se detallará sobre esta idea, conviene anotar que se trata de una afirmación coherente con lo ya expuesto, pues ha sido la capacidad y velocidad de agregación y procesamiento fruto de las nuevas tecnologías de computación lo que han permitido un mayor aprovechamiento de los datos e, incluso, que existan las *data driven companies*.

Visto todo lo anterior, estando de acuerdo la doctrina, los empresarios y las organizaciones no gubernamentales sobre la relevancia de los datos para el desarrollo de los negocios, conviene anotar que también se reconocen los diferentes retos que dicha postura comporta. El Fondo Monetario Internacional considera que la pregunta clave en torno a los datos personales debe ser sobre el acceso a los mismos, más que sobre la propiedad de estos[93]. Por el contrario, autores como Gates & Matthews y la consultora Baker Mckenzie, estiman que una de las problemáticas radica en la propiedad de los datos o bases de datos, en tanto activo empresarial[94].

92 Matthew Bodie et al. The Law and Policy of People Analytics. *University of Colorado Law Review*, 88(4). (2017). p. 3

93 Yan Carrière Swallow y Vikram Haksar The Economics and Implications of Data: An Integrated Perspective. (2019). https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

94 Carrie Gates y Peter Matthews. Data is the new currency. Paper presented at the *Proceedings of the 2014 New Security Paradigms Workshop*, (2014). p. 105-116.

Al afirmarse que los datos constituyen un activo empresarial que es objeto de transacciones económicas, se puede llegar al cuestionamiento de si es posible que estos formen parte del patrimonio y, por dicha vía, pueda protegerse el interés de los empresarios sobre estos. Empero, aun cuando dicho razonamiento encuentra fundamento desde la perspectiva gerencial, jurídicamente presenta más de una inquietud: De un lado, la pregunta central será si con la connotación constitucional a la que nos referiremos en el apartado siguiente, los datos en sí mismos son susceptibles de ser apropiados; o si, por el contrario, tras su procesamiento se pueden considerar como un producto independiente sobre el cual sí podría llegar a existir algún tipo de prerrogativa en cabeza del empresario. En segunda instancia, habría que preguntarse si tales intereses son susceptibles de ser protegidos mediante alguna de las categorías jurídicas ya existentes en el Derecho Privado.

Con ello en mente, a continuación se procederá a revisar la regulación actual sobre datos personales haciendo un paralelo entre la legislación colombiana y la comunitaria-europea.

1.8. Perspectiva jurídica

La disciplina de la protección de datos personales ha cobrado gran relevancia en tiempos recientes. No obstante, es importante resaltar cuál es el origen y fundamento de dicha protección con el fin de establecer el estado actual de la protección de datos personales de cara al uso y valor de estos en las transacciones comerciales.

1.8.1. Orígenes de la protección de datos personales

Para autores como Korff & Georges los conceptos de privacidad y protección de datos no son equivalentes, pues si bien se alimentan unos de otros, su distinción permite comprender el alcance de las normas de protección de datos personales[95]. Así, indican los mencionados autores que la génesis del concepto de privacidad se origina en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR en adelante por su nombre en inglés) y el artículo 8 de la Convención Europea de Derechos Humanos (ECHR en adelante por su nombre en inglés).

El artículo 8 del ECHR establece el derecho a la privacidad, en los siguientes términos:

> *"1. Toda persona tiene* ***derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia****.*

95 Douwe Korff, y Marie Georges. *The Origins and Meaning of Data Protection* (2020).

> 2. ***No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho*** *sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás"*[96].

Posteriormente, el artículo 17 del ICCPR recoge una redacción similar[97] a aquella del ECHR. Sin embargo, nótese que en ningún caso se hace referencia al derecho a la intimidad en relación con los datos personales.

Con posterioridad el Consejo de Europa promulgó la Convención 108 de 1981 para la Protección de las Personas frente al Procesamiento Automático de Datos Personales. El mencionado instrumento acogió el concepto del ICCPR y el ECHR sobre la privacidad e intimidad como Derecho Fundamental y adicionó un nuevo ingrediente normativo, al señalar lo siguiente "*(...)* ***con respecto al tratamiento automatizado de los datos de carácter personal*** *correspondientes a dicha persona" (*Negrilla fuera del texto original). Así, a criterio de autores como Guadamuz este constituye el primer antecedente directo de la protección de datos personales[98].

Tal reconocimiento normativo no fue fortuito, pues con el advenimiento de la computarización, la recolección y procesamiento de datos era cada vez más similar a las dinámicas que se conocen en la actualidad. En esa línea, la doctrina y la jurisprudencia dieron inicio a un largo camino en el estudio de lo que hoy denominamos protección de datos personales. Es, entonces, posible advertir que desde la perspectiva normativa los avances en la materia tienen un contenido esencialmente constitucional, orientado a la protección de la privacidad de las personas. Cabe cuestionarse si, como señala Janeček, la regulación está dispuesta sobre la base de la confusión entre el concepto de datos e información. Se ahondará sobre este punto más adelante.

Uno de los grandes hitos en la materia se dio a partir del asunto *Population Census Case* de 1983[99] conocido por el Tribunal Constitucional Federal Alemán, por medio de la cual se demandaba la inconstitucionalidad de la

96 Consejo de Europa. Convención Europea de Derechos Humanos (1950). https://www.echr.coe.int/documents/d/echr/convention_spa

97 El texto del artículo 17 del ICCPR señala: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"

98 Andrés Guadamuz. Habeas Data vs the European Data Protection Directive. *The Journal of Information, Law and Technology*, The Journal of Information, Law and Technology. (2001).

99 Laura Schertel Ferreira Mendes. Information Self-Determination and Habeas Data: Two Sides of the Same Coin? *Direitos Fundamentais & Justica, 39*, (2018). pp. 185-216. http://bases-biblioteca.uexternado.edu.co:2048/login?url=https://search.ebscohost.com/login.asp

Ley de Censo Poblacional de 1982 debido a los riesgos de la recolección y uso de dichos datos. El Tribunal declaró parcialmente inconstitucional la Ley de Censo Poblacional, arguyendo que, por virtud de los derechos al libre desarrollo de la personalidad y dignidad humana, era necesario permitir a las personas determinar qué información sobre sí mismos era accesible por terceros y con qué finalidad.

Dicha decisión dio paso a hablar sobre el Derecho a la Autodeterminación Informática, entendido como *"el poder del individuo en decidir por sí mismo sobre la recolección y utilización de sus datos personales"*[100-101]. Para autores como Hornung *et al.* la autodeterminación informática supone que los individuos estarán blindados de interferencias en sus asuntos personales, mientras que la protección de datos constituye una condición para la participación de los ciudadanos en procesos democráticos[102].

De otra parte, paralelamente también se ha desarrollado el concepto de *Habeas Data*, a criterio de autores como Pérez Luño[103] y Ferreira Laura esta noción apela al mecanismo procesal mediante el cual se puede salvaguardar el Derecho Fundamental a la Intimidad, aunque en muchas ocasiones se confunde esta expresión con el Derecho en sí mismo.

Los instrumentos internacionales a que se hizo referencia y la jurisprudencia alemana en el asunto *Population Census Case* de 1983 se erigieron como los primeros avances hacía la protección de datos personales tal y como se conoce en la actualidad, es decir, preservando, en su mayoría, el raigambre constitucional dirigido a la protección de la intimidad del individuo. Pese a ello, la regulación vigente también incorpora normas de derecho positivo que dan cuenta del reconocimiento de la economía basada en los datos. Acto seguido, se estudiará brevemente el estado de la regulación vigente en el ordenamiento comunitario europeo y el colombiano.

1.8.2. Autorización otorgada por el titular del dato personal

En atención al raigambre constitucional ya aludido, para la recolección y tratamiento de los datos de manera general los reguladores han optado por

x?direct=true&db=edshol&AN=edshol.hein.journals.direfnj39.10&lang=es&site=eds-live&scope=site

100 Ibíd.

101 Texto original : "o poder do individuo em determinar fundamentalmente por si mesmo sobre a coleta e utilizaçao de seus dados pessoais"

102 Hornung, Gerrit, y Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination". *Computer Law & Security Review* 25.1 (2009). pp. 84-88

103 Antonio Enrique Pérez Luño. Del habeas corpus al habeas data. *Informática Y Derecho: Revista Iberoamericana De Derecho Informático*, (1), (1992). pp. 153-161

establecer un sistema de autorización o consentimiento previo y expreso. Este sistema deriva de los presupuestos axiológicos sobre los que se cimienta la regulación, los cuales en términos generales son: i) que los datos se recolectan y procesan con una finalidad particular, ii) transparencia, iii) legalidad o licitud de dichos fines, iv) circulación restringida, entre otros.

Estos principios y esta exigencia de un consentimiento previo y expreso se encuentran consagrados en ordenamientos jurídicos colombiano y comunitario europeo. De una parte, el literal a) del artículo 3 de la Ley 1581 de 2012 define la autorización de la siguiente manera:

> *"a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;"*[104].

Posteriormente, el artículo 9 de este mismo cuerpo normativo establece la exigencia de dicha autorización para el tratamiento de los datos personales, indicando que deberá ser un consentimiento de carácter informado. Luego, ello supone que las finalidades del tratamiento deberán estar plenamente especificadas.

En consonancia con ello, el artículo 4 de esta misma Ley enuncia los principios para la interpretación y aplicación de las normas allí contenidas. Estos son: i) legalidad en materia de tratamiento de datos, ii) finalidad, iii) libertad, iv) veracidad, v) transparencia, vi) acceso o circulación restringida, vii) seguridad y viii) confidencialidad.

De otra parte, el RGPD también consagra disposiciones homólogas. En primera instancia, el artículo 4 (11) define el consentimiento del interesado en los siguientes términos:

> *"toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*[105].

Posteriormente, y de manera más extensa de lo que hace la Ley 1581 de 2012, el RGPD en su artículo 7 establece una serie de condicionamientos para la validez de dicho consentimiento. Igualmente, el artículo 5 de este cuerpo normativo enuncia los principios relativos al tratamiento. No obstante, a diferencia de lo que sucede en el ordenamiento jurídico colombiano, el

104 Congreso de la República de Colombia. [Ley 1581 de 2012]. Por la cual se dictan disposiciones generales para la protección de datos personales. (2012). [D.O.48.587]

105 Parlamento Europeo. Reglamento 2016/679: Reglamento General de Protección de Datos, (2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

RGPD no se limita a enunciarlos, pues desarrolla varios de ellos de manera individual, decantando su concepto[106].

Entonces, de acuerdo con lo expuesto el sistema de autorización supone que los titulares de datos consientan de manera previa, clara y expresa la recolección y tratamiento de sus datos, una vez han sido debidamente informados. Empero, aun cuando tal estrategia parece razonable de cara a garantizar el derecho a la autodeterminación informática, la naturaleza de los entornos digitales a través de los cuales se llevan un sinnúmero de actividades cotidianas supone grandes retos de cara a valorar la utilidad y efectividad del consentimiento.

De esta manera, el Big Data, la analítica de datos, los mercados de precio cero e, incluso, factores sociales han llevado a ciertos autores a considerar que un sistema de autorización para la recolección y tratamiento de datos es insuficiente de cara a las demandas del mundo comercial y tecnológico actual. También, debido a esa percepción de insuficiencia regulatoria y atendiendo a la utilidad y valor económico de esta *data*, algunos sectores empresariales han formulado opciones diferentes, como por ejemplo que los titulares de los datos sean pagados por la recolección y tratamiento de sus datos personales ¿Será ésta una nueva faceta de la autodeterminación informativa? Aun cuando tal cuestionamiento no tendrá una respuesta precisa en este punto de la evolución normativa y regulatoria, tales posturas resuenan con otros postulados como aquel de la Paradoja de la Privacidad, el cual se detallará brevemente más adelante.

Sin lugar a duda, actualmente el sistema de autorización o consentimiento constituye la columna vertebral del sistema regulatorio de protección de datos personales, el cual responde a una perspectiva eminentemente constitucional. Pese a ello, la regulación vigente también incorpora normas de derecho positivo que dan cuenta del reconocimiento de la economía basada en los datos. Acto seguido, se estudiará brevemente el estado de la regulación vigente en el ordenamiento comunitario europeo y el colombiano.

1.8.3. Ordenamiento jurídico colombiano

En el ordenamiento jurídico colombiano, la protección de datos como disciplina jurídica encuentra su fundamento en las normas constitucionales relativas al Derecho a la Intimidad. Esta protección surge del artículo 15 constitucional, el cual consagra el derecho a la intimidad como derecho fundamental, indicando que:

106 Al respecto ver artículo 7 y 12 del RGPD.

"Todas las personas tienen ***derecho a su intimidad personal y familiar*** *y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen* ***derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas****.*

En la ***recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*** *(...)"* (Negrilla fuera del texto original).

De igual manera, leyes estatutarias y ordinarias desarrollan este derecho, en concreto la Ley 1266 de 2008 relativa a la información financiera, crediticia y comercial; y, de otra parte, la Ley 1581 de 2012 como régimen general de protección de datos personales. Ambos cuerpos normativos destacan en su artículo 1º que el objeto de estas es:

"(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15º de la Constitución Política".

En esa misma línea, el Decreto 1377 de 2013, mediante el cual se reglamenta parcialmente la Ley 1581 de 2012, indica algunos parámetros relevantes sobre la autorización de uso que puede otorgar el titular, su revocabilidad y los derechos de los titulares.

Sin perjuicio de la connotación constitucional, tanto la Ley 1581 de 2012, como el Decreto 1377 de 2013, reconocen y regulan la transmisión y transferencia de datos, aunque no se establece definición legal para estas, por lo que, de manera general, debe entenderse que se trata del flujo o autorización de acceso a datos personales.

Tal reconocimiento también se hace patente en el informe de ponencia del proyecto de Ley 046 de 2010 contenido en la Gaceta del Congreso No. 1.023 del 02 de diciembre de 2010, puesto que se comienza justificando la propuesta a partir del reconocimiento de la importancia de los datos. Veamos:

"La sociedad moderna es una palpable representación de la importancia social y económica que tiene la información, los datos y su tratamiento, así permite entenderlo las siguientes cifras: el 18% de las compañías no hacen pública su política respecto de los datos personales, de los cuales disponen publicidad y ofertas en sus páginas, el 86% de los servidores usan 'cookies' , que registran los hábitos de consulta y otros datos de sus visitantes (...) Recientemente, los datos personales han sido tildados como "el nuevo petróleo de la internet y la nueva moneda del mundo digital"[107].

107 Congreso de la República de Colombia. Proyecto de Ley No.184 de 2010 Senado–046 de 2010 Cámara "Por la cual se dictan disposiciones generales para la protección de datos personales".

El reconocimiento de que existen negocios jurídicos que instrumenten dicha función económica supuso también un esfuerzo por regular la forma en que dichas operaciones deben efectuarse, las obligaciones para cada una de las partes y las limitaciones a las que se encuentra sometido el negocio de cara a no desproteger los intereses de los individuos cuyos datos están siendo transferidos o transmitidos. Es decir, que se ha impuesto límites claros a la autonomía privada en este aspecto, conduciendo a mantener un equilibrio en la protección de los datos personales de los individuos y los intereses de los empresarios sobre este nuevo insumo productivo.

Surge entonces la necesidad de discutir cuál es el tratamiento jurídico *ius privatista* que debe dársele a los datos ¿Cómo se protegen los intereses del empresario para el cual dichos datos son parte de su insumo productivo? Entendidos los datos recolectados y procesados como un insumo con valor empresarial. En esa línea, con el fin de analizar y contrastar los regímenes jurídicos aplicables, procederemos a estudiar el marco regulatorio comunitario de la Unión Europea sobre protección de datos personales.

1.8.4. Ordenamiento jurídico comunitario europeo

Las disposiciones que dan origen a la protección de datos en el sistema comunitario europeo son el artículo 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Particularmente, el artículo 8 del mencionado instrumento reconoce la protección de datos personales como un Derecho Fundamental autónomo, independiente del Derecho a la Intimidad. El mencionado artículo señala lo siguiente:

> *"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 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"*[108].

En un mismo sentido, el artículo 16 del Tratado de Funcionamiento de la Unión Europea reconoce también el Derecho a la protección de datos personales como derecho autónomo[109]. No obstante, la regulación sobre el particular no surge con el precitado instrumento, pues también reguló la materia el Convenio 108 mencionado previamente y la Directiva 95/46/CE, siendo

108 Parlamento Europeo. Reglamento 2016/679: Reglamento General de Protección de Datos, (2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

109 Tratado de Funcionamiento de la Unión Europea. (2012).

esta última derogada por la normatividad vigente a la que se hará referencia a continuación. Debe resaltarse que el Convenio 108 en su versión original de 1981 ya reconocía el flujo transfronterizo de datos, toda vez que dispuso algunas normas sobre este aspecto en el capítulo III.

En el año 2016 se expide el Reglamento General de Protección de Datos de la Unión Europea, el cual reglamenta el tratamiento de Datos Personales de cara a las normas precitadas y regula la libre circulación de estos. En todo caso, debe mencionarse que, al margen de la aplicabilidad directa del mencionado Reglamento, los Estados miembros cuentan con regulaciones nacionales, las cuales deben ajustarse a los parámetros del RGPD.

En punto a las transferencias de datos a nivel internacional, el RGPD se preocupa por mantener los estándares de protección para los titulares de los datos, al igual que la normatividad colombiana. Así pues, en el Capítulo V del Reglamento se incluyen diversas disposiciones tendientes a garantizar los estándares de protección cuando quiera que el tratamiento se haga fuera de la Unión Europea[110]. En ese sentido, se indica que en para transferencias a terceros países distintos a aquellos de la Unión Europea se hace necesario que:

> *i) "El país donde se ubica el receptor de la información cuente con estándares de protección adecuados (...);*
>
> *ii) El titular de los datos haya otorgado su consentimiento inequívoco para la transferencia;*
>
> *iii) Que la transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento de los datos, o para uno de otros fines específicos;*
>
> *iv) Que la transferencia verse sobre datos que son esencialmente públicos;*
>
> *v) Que exista un contrato entre el importador y exportador de datos donde, a opinión del regulador [nacional o comunitario], se brinden adecuadas garantías de seguridad por parte del importador"*[111].

Si bien dicha reglamentación encuentra una lógica coherente de cara a la protección de los Derechos Fundamentales de los titulares de los datos, es igualmente cierto que ante las prácticas del mercado como las mencionadas en acápites anteriores, tales pueden constituir una barrera para la

110 Al respecto puede observarse lo establecido en los artículos 44 y siguientes del RGPD, donde se establece, entre otros aspectos, el régimen de autorización que debe surtirse para las transferencias internacionales.

111 David Bender y Larry Ponemon. Binding corporate rules for cross-border data transfer. *Rutgers JL & Urb.Pol'Y, 3*, (2006). p.156.

negociabilidad de estos activos empresariales, especialmente en contextos de comercio transfronterizo.

En particular, el concepto de *"nivel adecuado de protección"* al que se refiere el artículo 4 del RGPD es un punto especialmente problemático frente a este punto, debido a lo cual la Comisión Europea ha debido proferir decisiones de implementación sobre los niveles adecuados de protección de datos personales en el marco de la privacidad de datos de la Unión Europea y los Estados Unidos de Norte América, en la que se regula de manera específica las condiciones para que las empresas certifiquen tener unos niveles adecuados de tratamiento y no se socaven los derechos fundamentales de los titulares de estos datos[112]. En todo caso, conviene anotar que dicha Decisión acogió las posturas del Tribunal de Justicia de la Unión Europea cuando señaló en el caso Maximilian Scrhems v. Data Protection Comissioner que los niveles adecuados de protección no comportan igualdad o exactitud en los medios de protección respecto del RGPD. A juicio personal, dicha postura es conveniente y oportuna, como quiera que propende por facilitar el intercambio comercial de datos, sin deteriorar las garantías otorgadas a los titulares de los datos.

Revisada y analizada la literatura anterior, al igual que las entrevistas practicadas, se han hecho patentes las zonas grises de la regulación a las que se enfrenta el uso y aprovechamiento de datos personales para la actividad empresarial. No obstante lo anterior, también se ha puesto de presente la utilidad que reviste la recolección y analítica de datos y los impactos de mercado que esto supone.

Así, con esta perspectiva, procede referirnos a la metodología de investigación que orientó la elaboración de este escrito y, posteriormente, entrar a dar respuesta a la pregunta central de investigación: ¿Cómo pueden los empresarios proteger los datos personales usados como insumo de la actividad empresarial?

2. METODOLOGÍA DE LA INVESTIGACIÓN

El presente trabajo de investigación parte del siguiente presupuesto: Tal y como lo indica el Foro Económico Mundial, los datos son el nuevo petróleo, erigiéndose como un nuevo factor de producción[113]. Entonces, en las diná-

112 Sobre el particular ver Decisión de Implementación de la Comisión Europea de 10 de julio de 2023, relativa a la regulación 2016/679 del Parlamento Europeo y el Consejo sobre el nivel adecuado de protección de datos personales bajo el marco de la Protección de Datos ente la Unión Europea y los Estados Unidos de Norte América. Enlace de consulta: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

113 Foro Económico Mundial, & Bain & Company Inc. Personal data : The emergence of a new asset class. (2011). https://www3.weforum.org/docs/

micas actuales del mercado los datos cobran una especial relevancia para el desarrollo de la actividad empresarial.

De otra parte, desde el escenario jurídico se evidencia la preminencia de una regulación entorno a los datos personales que tiene como objetivo proteger y garantizar la defensa del derecho a la privacidad e intimidad de los titulares de los datos. Sin embargo, cabe analizar si el empresario puede proteger estos datos, especialmente datos personales, como lo haría con cualquier otro activo relevante para su negocio. Así las cosas, partiendo de las premisas señaladas, la presente investigación tiene como objeto central dar respuesta al siguiente cuestionamiento ¿Puede el empresario proteger los datos personales como insumo de su actividad empresarial?

Para ello, en la presente investigación se utilizó una metodología socio-jurídica, en donde se procuró dar respuesta al interrogante de manera interdisciplinar, esto es, acudiendo a una perspectiva jurídica y gerencial. De igual forma, para tal fin se hizo imperativo practicar trabajo de campo a través de entrevistas, las cuales tienen como propósito brindar una perspectiva pragmática a la discusión y evaluar los matices de este cuestionamiento a la luz de las dinámicas actuales del mercado.

El escrito toma como base la información recopilada, analizada y contrastada en la revisión de literatura, a partir de la cual se pudo obtener valiosas conclusiones sobre la relevancia de los datos en el entorno empresarial y los razonamientos existentes detrás de las disposiciones que regulan el tratamiento de datos personales.

A partir de tales conclusiones, el texto del trabajo busca establecer cuál es la categoría de protección jurídica que permitiría al empresario proteger sus intereses, de existir, denotando su viabilidad -o no-, así como las potenciales ventajas o limitaciones que su aplicación supondría. Para ello, se efectúa la revisión de dichas categorías jurídicas en relación con los diferentes estadios de la *data* en la cadena de valor, es decir, reconociendo la existencia de un mercado de datos.

De igual manera, las categorías jurídicas propuestas se evalúan desde la regulación vigente en Colombia y, en algunos casos, se contrasta con normativa comunitaria de la Unión Europea, con el fin de establecer puntos de contraste valiosos para la discusión. Por contera, desde el estudio realizado de cada categoría jurídico se establecen unas conclusiones que permiten dar respuesta a la pregunta de investigación propuesta y, adicionalmente, hacer algunas anotaciones sobre el tratamiento *ius privatista* que de facto se da a los datos personales.

WEF _ ITTC _PersonalDataNewAsset_Report_2011.pdf

3. ¿CÓMO PUEDE EL EMPRESARIO PROTEGER LOS DATOS PERSONALES QUE SON INSUMO DE SU ACTIVIDAD?

El presupuesto del que parte el presente trabajo de investigación es que los datos son un insumo y/o activo de gran relevancia y utilidad para el empresario. Como se expuso a lo largo de la revisión de literatura que antecede, dicha apreciación no es aislada ni infundada. Para el Foro Económico Mundial los datos se han convertido en una nueva materia prima, equiparables a factores de producción como el capital y el trabajo. El mundo se dirige hacia una regulación donde se tengan en cuenta los intereses de todos los actores, esto es, los titulares de los datos y el sector público y privado[114].

La literatura analizada y las entrevistas practicadas dan cuenta del rol protagónico que han tomado los datos en la economía digital y que el norte de la regulación debe ser la búsqueda de un punto equilibrado en lo que refiere a la protección de los intereses de los titulares y la libre circulación de los datos como parte del engranaje productivo.

Es preciso aclarar que una postura que favorezca el uso de los datos personales en la actividad empresarial no implica pretender disminuir los niveles de protección de la privacidad. Por el contrario, las entrevistas practicadas revelaron que es de interés del empresariado enviar a los consumidores y al público en general un mensaje de seguridad, confianza y transparencia a los titulares de datos sobre su utilización, contrario al imaginario colectivo.

Respecto de este último punto también conviene hacer unas breves anotaciones. Distintas obras a propósito del uso de los datos personales se concentran en señalar los usos indebidos o abusos en la utilización de estos datos por parte de las empresas y del sector público. Se parte de un presupuesto: Las empresas y el sector público recolectan los datos personales para controlar y vigilar a los individuos. Empero, se deja de lado también los beneficios que dicha recolección y uso de datos conlleva, entre los que se destaca la generación de eficiencias[115], la creación de nuevos productos y a nivel macroeconómico el desarrollo de todo un nuevo sector dedicado a la recolección, limpieza y análisis de datos.

Ante tal disyuntiva la pregunta que surge es ¿Por qué ante la preocupación sobre la privacidad no se evidencia que los consumidores emprendan medidas idóneas para proteger sus datos personales? Pues bien, partiendo de la premisa de que los consumidores otorgan libremente sus datos y posteriormente manifiestan preocupación por su uso y el resguardo de su privacidad,

114 Foro Económico Mundial, & Bain & Company Inc. Personal data: The emergence of a new asset class. (2011). https://www3.weforum.org/docs/WEF _ ITTC _PersonalDataNewAsset_Report_2011.pdf

115 Ibid.

es decir, de la existencia de un patrón de conducta inconsistente o contradictorio de los consumidores; la doctrina ha estudiado esta dinámica que ha denominado la paradoja de la privacidad *(the privacy paradox)*.

En otros términos:

> *"[Este planteamiento] describe la dicotomía entre la actitud y el comportamiento real respecto de la privacidad de la información. (…) Por un lado, los usuarios expresan su preocupación por el tratamiento de sus datos personales y manifiestan su deseo de protegerlos, mientras que, al mismo tiempo, no sólo ceden voluntariamente estos datos personales al publicar detalles de su vida privada en las redes sociales o utilizar rastreadores de actividad física y sitios web de compras en línea que incluyen funciones de elaboración de perfiles, sino que rara vez se esfuerzan por proteger sus datos de forma activa, por ejemplo mediante la eliminación periódica de cookies o el cifrado de sus comunicaciones por correo electrónico"*[116]

Son distintas las justificaciones usadas para explicar esta dinámica. Entre las más relevantes se encuentran la búsqueda de la maximización de los beneficios reportados por la entrega y uso de dichos datos, la existencia de sesgos que limitan la capacidad de tomar una decisión informada, la falta de conocimiento técnico sobre medidas para proteger su privacidad, la influencia social, entre otras[117]. Con este postulado el proteccionismo de datos parece perder sentido, pues *"la incoherencia entre la actitud hacia la privacidad y el comportamiento real debilita esta justificación"*[118].

En todo caso, vale la pena resaltar que la paradoja de la privacidad es un asunto ampliamente debatido aún, pues como lo resalta Kokolakis la

116 Nina Gerber, et al. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *In Computers and Security* (Vol. 77). (2018). pp. 227. https://doi.org/10.1016/j.cose.2018.04.002. Traducción libre.Texto original: *"which describes the dichotomy of information privacy attitude and actual information privacy behavior. (…) On the one hand, users express concerns about the handling of their personal data and report a desire to protect their data, whereas at the same time, they not only voluntarily give away these personal data by posting details of their private life in social networks or using fitness trackers and online shopping websites which include profiling functions, but also rarely make an effort to protect their data actively, for example through the deletion of cookies on a regular basis or the encryption of their e-mail communication"*.

117 Nina Gerber, et al. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *In Computers and Security* (Vol. 77). (2018). pp. 227. https://doi.org/10.1016/j.cose.2018.04.002.

118 Spyros Kokolakis. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, (2017). pp. 122–134. Texto original: *"The privacy paradox has significant implications for e-commerce, e-government, online social networking, as well as for government privacy regulation. E-commerce and online social networking sites are collectors of vast amounts of personal information. A proof of the privacy paradox would encourage them to increase the collection and use of per- sonal information. Government policy makers, on the other hand, justify privacy regulation on people's raised privacy con- cerns. The inconsistency between privacy attitude and actual behaviour weakens this justification"*.

evidencia aún no es contundente. Incluso, autores como Solove destacan que esta paradoja es aparente[119].

Ahora bien, retornando a la perspectiva del empresario en la utilización de datos personales, es prudente también resaltar que este afronta varias dificultades en el uso de los datos para su actividad, entre las que encontramos: i) la obsolencia de la regulación de protección de datos personales; ii) las zonas grises de la regulación y iii) la complejidad y diversidad de regímenes de protección de datos en una economía digital globalizada.

Frente a la segunda inquietud, existe especialmente de un punto generador de incertidumbre que resulta nuclear: la ambigüedad de la definición de datos personales. Tal y como se expuso en la revisión de literatura, las definiciones estrictamente legales de datos personales son bastante amplias, lo que ubica a los empresarios en una zona gris donde no se tiene claridad si se está incurriendo en una infracción a la normativa de protección de datos. Asimismo, esfuerzos como el de la OCDE en tratar de enlistar qué tipos de datos se pueden considerar como personales, coadyuvan a esta ambigüedad. A su vez, dicha incertidumbre se exacerba si se considera que la mayoría de los datos son tratados y analizados en conjunto, por lo que el análisis integral de los mismos puede conllevar a que con estos se haga posible la identificación de una persona y, en consecuencia, se trate de un dato personal.

Entendida la postura del sector privado respecto de la relevancia y utilidad de los datos en la actividad productiva, cabe cuestionarse ¿Debe darse un tratamiento jurídico *ius privatista* a los datos personales como insumo productivo del empresario? La presente investigación partirá de dos presupuestos. Primero, la libre circulación de los datos es un escenario deseable para el mercado. Segundo, en efecto los datos recolectados, procesados y utilizados por el empresario para el desarrollo de su actividad deben ser protegidos como cualquier otro insumo y/o factor productivo, dada su importancia en la actividad empresarial contemporánea.

¿Cuál debe ser la protección que deben tener los datos usados por el empresario para el desarrollo de su actividad? ¿Existe una categoría jurídica de derecho privado que permita proteger el interés del empresario sobre estos datos? El presente escrito abordará estos cuestionamientos desde una óptica interdisciplinar o socio-jurídica, es decir, acudiendo a revisar los aspectos prácticos del tema y las perspectivas gerenciales y económicas a que haya lugar.

A continuación se estudiará el objeto de protección para, posteriormente, analizar las categorías jurídicas que permiten la protección de estos intereses en cabeza de los empresarios. Cabe anotar que la presente investigación no pretende proponer soluciones jurídicas diferentes a las ya contempladas en el

119 Solove, Daniel J. The Myth of the Privacy Paradox. George Washington Law Review, 89(1). (2021). https://doi.org/10.2139/ssrn.3536265

derecho positivo, por lo que se dará respuesta a la pregunta de investigación a partir de la revisión de las categorías jurídicas existentes y vigentes actualmente, revisando para el efecto la legislación colombiana y el ordenamiento jurídico comunitario europeo, principalmente.

3.1. ¿Cuál es el objeto de protección?

¿Es el dato en bruto, el dato agregado o el dato analizado lo que más interesa al empresario? ¿Cuál es el real objeto merecedor de protección?

Las entrevistas practicadas señalan que es el dato analizado aquel que tiene valor y utilidad para el empresario. Se evidencia particularmente en la entrevista obrante en el Anexo No. 2, que la verdadera utilidad de la información extraída de los datos personales resulta de un arduo proceso de limpieza, depuración y análisis, sin el cual no sería posible utilizarla efectivamente para la toma de decisiones gerenciales.

En consecuencia, para responder al interrogante planteado en este acápite debe distinguirse los estados de la *data*, puesto que ello permite identificar objetos de protección diferentes. Así, la cadena de valor de los datos se estructura en cuatro fases: i) generación, ii) recolección, iii) análisis y iv) intercambio[120].

En la fase de generación se encuentran los datos en bruto, es decir, sin ningún tipo de intervención. Si bien en este estado los datos tienen una potencialidad para ser utilizados, en este estadio es poco lo que se puede aprovechar de estos. No obstante, es claro que se trata del insumo para las siguientes etapas de cadena de valor, por lo tanto, es válido examinar si estos son susceptibles de ser protegidos desde la perspectiva del derecho mercantil.

Posteriormente, en su fase de recolección los datos son depurados y, en algunos casos, transformados, organizados y almacenados[121]. Una vez los datos han pasado por estos procesos puede existir un nuevo producto distinto al dato en bruto, tales como las bases de datos. Con posterioridad observaremos que estas bases de datos, aun las que incluyen datos personales, constituyen un objeto de protección independiente sobre el cual ya existe una categoría jurídica para protegerlas.

La fase de análisis es la más importante de la cadena de valor[122].Como resultado de las acciones desarrolladas en esta etapa de la cadena de valor,

120 Zakaria Faroukhi, et al Big data monetization throughout Big Data Value Chain: a comprehensive review. *Journal of Big Data*, 7(1). (2020). https://doi.org/10.1186/s40537-019-0281-5

121 Zakaria Faroukhi, et al Big data monetization throughout Big Data Value Chain: a comprehensive review. *Journal of Big Data*, 7(1). (2020). https://doi.org/10.1186/s40537-019-0281-5

122 Ibid. p.5.

tras un proceso de evaluación crítica y analítica los datos revelan información. El resultado de esta valoración de los datos y la información que representan puede también ser un producto independiente. Piénsese en el caso de los negocios que venden el servicio de analítica de datos o métricas de sitios web, tales como Google Analytics o Leadfeeder.

La comprensión de la cadena de valor de los datos permite establecer que, tanto los datos como los productos derivados de estos, son relevantes para el empresario y pueden constituir objetos de protección jurídica independientes a los cuales les serán aplicables distintas categorías jurídicas.

Con esto en mente, a continuación se revisarán distintas categorías jurídicas de protección frente a las cuales se buscará determinar su aptitud para proteger alguno de los tres estados de los datos a los que se hizo referencia en este acápite. Asimismo, se establecerán las consecuencias jurídicas de la aplicación de cada una de estas categorías.

3.2 ¿Pueden ser los empresarios propietarios de los datos que recolectan?

Vláclav Janeček[123] puso sobre la mesa la discusión sobre la propiedad de los datos personales generados por el Internet de las Cosas. El texto pone de presente algunas dificultades que anteceden a revisar el tratamiento jurídico de los datos como activos. Una de estas dificultades consiste en el hecho de que el Internet de los Datos genera metadatos, los cuales según lo expuesto en la revisión de literatura pueden ser considerados y tratados como datos personales. Para el autor, la distinción entre el concepto de dato e información resulta ser un aspecto nuclear en lo que refiere a la determinación de un tratamiento jurídico de los datos como activos empresariales. Pese a que definitivamente se trata de conceptos distintos, a juicio personal no es posible ontológicamente escindir la información del dato que la contiene, lo que supone dificultades para partir de tales distinciones para el diseño regulatorio.

Sin pretender exceder los límites de esta investigación, desde otra perspectiva también conviene anotar que el concepto de identificabilidad al que se refieren las definiciones legales sobre datos personales implica igualmente una serie de retos y vicisitudes de cara a determinar una categoría jurídica que proteja el interés de los empresarios sobre los metadatos, tales como datos de navegación, preferencias, leads, etc. Estos datos son de especial relevancia para el despliegue de actividades de mercadeo y publicidad pero, al estar asociados a una dirección IP o un usuario, son susceptibles de ser considerados como datos personales; sin embargo, ¿Permiten estos la identificación real

123 Vláclav Janeček. Ownership of personal data in the Internet of Things. Computer Law and Security Review, 34(5). (2018). https://doi.org/10.1016/j.clsr.2018.04.007

de una persona? ¿Su protección como datos personales conlleva a proteger el núcleo esencial del derecho a la intimidad o la privacidad de los seres humanos? Reconociendo que estos son cuestionamientos amplios y que se separan de la pregunta de investigación planteada, se limitará a dejar planteada esta inquietud para próximas investigaciones.

Para dar respuesta a la pregunta planteada, se comenzará por estudiar la aptitud de la categoría jurídica del derecho real de dominio para proteger el interés del empresario sobre los datos. Se estudiará su aplicabilidad sobre los datos en la etapa de generación de la cadena de valor. Posteriormente, se hará referencia a los datos en etapa de recolección y análisis, incluyendo al estudio otras categorías jurídicas relevantes para esta investigación.

3.3. Derecho de Dominio sobre los datos personales

El artículo 653 del Código Civil Colombiano define el concepto de *bien* para introducir la regulación a propósito de los Derechos Reales, de la siguiente forma:

> *"Los bienes consisten en cosas corporales o incorporales. Corporales son las que tienen un ser real y pueden ser percibidas por los sentidos, como una casa, un libro. Incorporales las que consisten en meros derechos, como los créditos y las servidumbres activas".*[124]

Este es un primer punto de discusión para poder hablar de los datos, ¿Son los datos un bien? Es claro que a partir del concepto de corporalidad no. Sin embargo, más adelante se analizará la naturaleza de los datos respecto del concepto de bienes incorporales y la posibilidad de aplicar las categorías jurídicas de la Propiedad Intelectual.

Ahora bien, el artículo 665 del mismo cuerpo normativo nos brinda la noción de Derecho Real, al señalar lo siguiente:

> *"Derecho real es el que tenemos sobre una cosa sin respecto a determinada persona.*
>
> *Son derechos reales el de dominio, el de herencia, los de usufructo, uso o habitación, los de servidumbres activas, el de prenda* y el de hipoteca. De estos derechos nacen las acciones reales*[125].

Los Derechos Reales son definidos como un poder o potestad sobre una cosa y el legislador estableció un listado taxativo de los derechos reales que pueden existir sobre las cosas. En ese listado, se encuentra el Derecho de Dominio, definido por el artículo 669 en los siguientes términos:

124 Congreso de La República de Colombia. Ley 57 de 1887. (Código Civil)
125 Congreso de La República de Colombia. Ley 57 de 1887. (Código Civil).

> *"El dominio que se llama también propiedad es el derecho real en una* ***cosa corporal****, para gozar y disponer de ella, no siendo contra ley o contra derecho ajeno. La propiedad separada del goce de la cosa se llama mera o nuda propiedad"*[126] (Negrilla fuera del texto original).

Entonces, la primera limitación para poder hablar de un derecho de propiedad sobre los datos es su corporeidad, pues no se trata de un bien corporal sobre el cual sea susceptible ejercer un Derecho de Dominio. En la misma línea, respecto de la protección de los datos personales en poder del empresario no encuentra cabida otro Derecho Real de los mencionados por el artículo 665 precitado, pues se trata de un sistema de *numerus clausus*.

Aunado a lo anterior, el Derecho de Dominio, en tanto facultad o poder sobre un objeto, se traduce en una consecuencia jurídica: El ingreso de ese bien corporal al patrimonio de quien ostenta el Derecho de Dominio. Bajo esa lógica, no es posible concebir que el dato en bruto sea susceptible de ingresar al patrimonio, aún si se parte de la distinción entre dato e información. A propósito de este asunto Janeček sugiere lo siguiente:

> *"Se puede argumentar que, desde un punto de vista ontológico, estos datos son constitutivos de la propia identidad, porque "no hay diferencia entre la esfera informativa [interpretada por estos datos intrínsecamente personales] y la identidad personal". Por tanto, la propiedad de estos datos implicaría conceptualmente la propiedad de la identidad de las personas"*[127].

A partir de lo esbozado resulta diáfano que no es posible hablar de la existencia de Derecho Real de Dominio sobre los datos personales en su etapa de generación, es decir, sobre el dato en estado bruto y sin modificación alguna. A su vez, dada la falta de corporeidad de los datos recolectados, procesados y analizados, tampoco es posible aplicar esta categoría jurídica a estadios más avanzados de la *data*. Empero, conviene analizar la aplicabilidad de las categorías jurídicas de la Propiedad Intelectual, en tanto forma de propiedad especial.

3.3. La Propiedad Intelectual y los datos personales

El objeto de esta disciplina es la regulación jurídica de la producción intelectual[128]. Surge entonces el primer cuestionamiento ¿Son los datos personales una producción del intelecto humano? Para responder a este cuestionamiento nuevamente es necesario referirnos a los distintos estados de los datos dentro de la cadena de valor.

126 Ibíd.

127 Vlacav Janeček, "Ownership of personal data in the Internet of Things", Computer Law and Security 34, n. º 5 (2018). p. 8 https://doi.org/10.1016/j.clsr.2018.04.007

128 Daniel Stengel. La propiedad intelectual en la filosofía. Revista La Propiedad Inmaterial, 8, (2004) pp. 71-106.

Respecto de los datos personales en su estado de generación, esto es, en el momento de su creación activa o pasiva por parte de los individuos[129], no se logra advertir que exista intervención del intelecto humana que pueda conllevar a calificarlo como una creación intelectual. Es decir, al hablar del dato en bruto no es posible concebirlo como una producción intelectual susceptible de ser protegido mediante el sistema de patentes y/o a través del Derecho de Autor.

Un primer motivo que respalda esto es que los datos en bruto corresponden a una representación de hechos, bien sea que estos hayan sido generados de manera activa por el individuo -es decir mediante su entrega voluntaria- o pasivamente – por la navegación o uso de un sistema electrónico. De esta forma, siendo que no corresponden a una invención humana, no es dable aplicar las categorías de protección del régimen de Propiedad Intelectual.

Ahora bien, haciendo caso omiso de lo anterior, de analizarse la aplicabilidad de las patentes de invención para proteger los datos se encontraría igualmente un resultado negativo. Veamos:

De conformidad con el artículo 14 de la Decisión 486 de 2000, las patentes de invención deben reunir los siguientes requisitos: i) novedad, ii) altura inventiva y iii) que sean susceptibles de aplicación industrial. Resulta claro que los datos no reúnen alguno de estos requisitos, debido a que no pueden ser considerados como una producción del intelecto humano que, adicionalmente, sean novedosos y no se encuentran previamente en el estado del arte; todo lo anterior como quiera que son, sencillamente, una representación de hechos.

Lo mismo se predica de los datos en su estado de recolección y análisis, es decir, una vez estos han sido organizados, dispuestos de una manera particular y se ha obtenido conclusiones sobre determinados hechos a partir de ellos; esto es, cuando estos han sido incorporados en una base de datos. De esta forma, en tanto no constituyen una invención, de manera expresa el literal f) del artículo 15 de la Decisión 486 de 2000 excluye expresamente su consideración como patentes de invención: *"No se considerarán invenciones: (…) f) las formas de presentar información"*.

También desde la óptica de las patentes de invención habrá que referirse someramente a la protección de los sistemas utilizados para el procesamiento y analítica de datos. Lo primero que se debe anotar es que, dado que se trata de un producto independiente a los datos que procesa y analiza, el estudio de los medios de protección aplicables se orientará eminentemente a las categorías de la Propiedad Intelectual. Hecha esa aclaración, son dos las

129 Zakaria Faroukhi, et al. Big data monetization throughout Big Data Value Chain: a comprehensive review. *Journal of Big Data*, 7(1). (2020). https://doi.org/10.1186/s40537-019-0281-5

figuras meritorias de ser analizadas para este fin: las patentes de invención y el derecho de autor.

El artículo 15 de la Decisión 486 de 2000 relaciona lo que no se podrá considerar como una invención patentable, entre lo que se incluye a los programas de ordenador o software. Es decir, los programas de ordenador y softwares en sí mismos, no podrán ser considerados una invención y ser patentables. Esta disposición está en consonancia con lo dispuesto por el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC en adelante), puesto que allí se señala que la protección aplicable es la del Derecho de Autor. Aun cuando tal aspecto no ha sido pacífico y las regulaciones a nivel global no son uniformes, Colombia ha acogido este concepto a través de la mencionada Decisión Andina. Luego, en el escenario colombiano al hablar de los sistemas que sirven para la analítica de datos – en principio- el análisis sobre su protección jurídica deberá hacerse de cara a las normas del Derecho de Autor contenido en la Decisión 351 de 1993. En todo caso, conviene anotar que tal análisis refiere específicamente al programa de ordenador y no a los datos que lo alimentan, cuestión que difiere de los aspectos que se precisan a continuación.

Respecto de los datos en bruto o en estado de generación, tampoco es dable una protección desde el Derecho de Autor. El dato en esta etapa de la cadena de valor no reúne los requisitos para ser protegido como una obra, los cuales son: i) originalidad, ii) que sea una creación proveniente del intelecto humano y iii) que esté fijado en un soporte material. Como se aprecia, la dificultad de calificar al dato como una obra estriba, principalmente, en la satisfacción de los dos primeros requisitos, habida cuenta de la ausencia de intervención intelectual humana.

Pese a lo anterior, es posible encontrar una vía de protección en estadios más avanzados de la cadena de valor, esto es, cuando los datos han sido dispuestos y organizados de tal forma que han devenido bases de datos. Dicha protección se encuentra circunscrita y limitada. Para el caso colombiano, este aspecto se encuentra disciplinado tanto por el ADPIC, como por la Decisión Andina 351 de 1993, la cual regula los Derechos de Autor y Conexos. Veamos:

El numeral 2 del artículo 10 del ADPIC señala:

> *"Las compilaciones de datos o de otros materiales, en forma legible por máquina o en otra forma,* ***que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual****, serán protegidas como tales.* ***Esa protección, que no abarcará los datos o materiales en sí mismos****, se entenderá sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales en sí mismos"* (Negrilla fuera del texto original).

Por su parte, el artículo 4 la Decisión Andina 351 de 1993 dispone:

> *"La protección reconocida por la presente Decisión recae sobre todas las obras literarias, artísticas y científicas que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocer, y que incluye, entre otras, las siguientes: (…) ll) Las antologías o compilaciones de obras diversas y las bases de datos,* ***que por la selección o disposición de las materias constituyan creaciones personales***" (Negrilla fuera del texto original).

Tal y como se desprende de los artículos precitados, la protección otorgada por el Derecho de Autor versa sobre los aspectos de la selección o disposición del contenido, pues es precisamente allí donde radica la originalidad necesaria para ser procedente la protección como obra. En ambos casos dicha protección excluye los datos individualmente considerados, lo cual es coherente con los principios de este régimen de protección y con las anotaciones hechas con anterioridad.

Pese a la relevancia de tal protección, al versar exclusivamente sobre los aspectos de selección y organización del contenido permanece la inquietud sobre cómo podría el empresario proteger la información allí contenida de una sustracción total o parcial no autorizada. El espectro limitado de esta protección hace pertinente considerar otras categorías jurídicas de protección y analizar su aplicabilidad. Con fundamento en ello, conviene preguntarse ¿Pueden considerarse los datos personales de individuos vinculados directa o indirectamente con una empresa como información secreta? A continuación, se estudiará la protección jurídica de los datos personales como insumo empresarial por vía de los secretos empresariales:

3.4. Los secretos empresariales y los datos personales:

En el ordenamiento jurídico colombiano los secretos empresariales son regulados por la Decisión 486 de 2000. En particular, el artículo 260 de ésta los define de la siguiente forma: *"(…) cualquier* ***información no divulgada*** *que una persona natural o jurídica legítimamente posea, que* ***pueda usarse en alguna actividad productiva, industrial o comercial****, y que sea susceptible de transmitirse a un tercero (…)*" (Negrilla fuera del texto original).

Si bien esta definición no especifica que los datos personales sean susceptibles de ser considerados como un secreto empresarial, de acuerdo con lo expuesto a lo largo de este escrito, el concepto de información abarca también los datos personales de los consumidores o trabajadores.

A modo de guisa, esta comprensión es incorporada de manera más explícita en la Directiva 2016/943 del Parlamento Europeo, la cual en las consideraciones No. 2, 34 y 35 hace alusión a los datos personales de distintos actores asociados con la actividad empresarial como parte de los datos comerciales que no constituyen desarrollos técnicos o científicos protegibles por vía de

la Propiedad Intelectual[130]. Luego, en principio, por el objeto de la materia que comprende el secreto industrial no existiría una limitación para la protección de los datos personales mediante esta categoría jurídica.

Ahora bien, más adelante el precitado artículo de la Decisión 486 de 2000 relaciona tres (3) requisitos para considerar la información como secreto empresarial. Estos requisitos son: i) su calidad de secreta, dada por el nivel de accesibilidad a esta por terceros, ii) su valor económico y iii) las medidas para mantener secreta dicha información. Veamos la satisfacción de estos requisitos para la protección de los datos personales:

Respecto del valor económico de esta información, no existe duda de que los datos personales recolectados por las empresas entrañan un valor económico y una utilidad para el empresario, tal y como se ha expuesto *in extenso* en este escrito. En punto al requisito de accesibilidad, dada la regulación de protección de datos personales, especialmente las disposiciones derivadas del principio de acceso y circulación restringida concretadas en la determinación de sujetos responsables del tratamiento, es posible predicar la satisfacción de este requisito. Frente al cumplimiento del tercer requisito, *prima facie* los principios de confidencialidad y seguridad orientarían la implementación de medidas razonables para la seguridad, por lo que en principio este requisito también se encontraría satisfecho.

Empero, el análisis sobre estos elementos no es pacífico. El artículo 261 de la Decisión 486 de 2000 precisa lo siguiente: *"A los efectos de la presente Decisión, no se considerará como secreto empresarial aquella información que deba ser divulgada por disposición legal o por orden judicial"*. Surgen entonces diversos cuestionamientos sobre la satisfacción de los requisitos anteriores ¿Es el Derecho de acceso a sus datos en cabeza los titulares[131] óbice para considerar esta información como secreto empresarial? En atención estricta a lo dispuesto por el artículo precitado sí y, en consecuencia, no sería susceptible de ser protegida mediante el secreto empresarial. ¿Esta disposición refiere a la divulgación de la información considerada en su conjunto o de manera individual y particularizada? El literal a) del artículo 260 refiere que: *"(…) dicha información sea: a) secreta, **en el sentido que como conjunto o en la configuración y reunión precisa de sus componentes**, (…)"*, por lo que cabe también una interpretación favorable a considerar que la concesión de este derecho, y su ejercicio por parte de los titulares de los datos, no impediría la aplicabilidad de esta categoría jurídica.

130 Parlamento Europeo. Directiva 2016/943. (2016).

131 Para el efecto, debe recordarse que en la legislación colombiana el literal f) del artículo 8 de la Ley 1581 de 2012 establece el derecho de los titulares a acceder a sus datos personales que hayan sido objeto de tratamiento. Veamos: *"El Titular de los datos personales tendrá los siguientes derechos: f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento"*.

En suma, conviene analizar la presencia de estos elementos de manera individual en cada caso. A modo de ejemplo, en la entrevista obrante en el Anexo No. 2 la discusión versa sobre los datos personales de los trabajadores de la empresa. Si bien en líneas anteriores se destacó la utilidad de estos datos para generar mayores eficiencias en los procesos internos de la organización, es posible que algunos no consideren que estos datos tengan una valoración económica, toda vez que no redundan de manera directa en una actividad comercial de la empresa.

Ahora, como quiera que el concepto de información al que se refiere la definición de secreto empresarial es más amplio que la noción de *base de datos* a la que se hizo referencia en el acápite anterior, no se hace imperativa la distinción sobre la etapa en que se encuentra la data en la cadena de valor. Así, una ventaja que presenta esta categoría jurídica para la protección de los datos personales es que puede encontrarse en su estado más primigenio, o por el contrario ya dispuesta y seleccionada, e igualmente podría analizarse su protección bajo esta figura.

Pese a no ser del todo clara la protección que pueda darse a los datos personales en tanto insumo empresarial, sí es claro que en el ordenamiento jurídico colombiano la aplicabilidad del secreto industrial no opera en detrimento de los derechos y garantías establecidos en el régimen de protección de datos. Por lo tanto, se trata de una alternativa interesante y versátil para la protección de los datos personales como activo, aunque, como se anotó, hace falta mayor claridad respecto de algunos conceptos asociados a esta figura, de cara también a la búsqueda de un balance entre la protección de ambos intereses.

Al margen de lo anterior y en gracia de discusión, es oportuno hacer referencia a un Derecho *sui generis* del ordenamiento jurídico comunitario europeo, a través del cual se protege el contenido de las bases de datos y no su sola disposición y selección. En el siguiente acápite se expondrá brevemente esta figura, en tanto referente de derecho extranjero pertinente para el objeto de esta investigación.

3.5. La Directiva 96/9/CE sobre la protección jurídica de las bases de datos

Como lo indica el propio título de la Directiva, el objeto de protección supone que la *data* se encuentre en un estado más avanzado al interior de la cadena de valor, esto es, ya recolectada, seleccionada y organizada constituyendo una base de datos.

Previamente a hacer alusión al contenido normativo de la Directiva, se precisa comprender las motivaciones detrás de este instrumento jurídico. Para comenzar, en sus consideraciones reconoce la insuficiencia en la protección de las bases de datos, específicamente en los ámbitos de la Propiedad

Intelectual, así como la disparidad de niveles de protección en los distintos Estados de la unión.

A partir de lo anterior, el Parlamento Europeo y el Consejo de Europa estiman en la consideración No. 6 hace referencia a la necesidad de proteger el contenido de las bases de datos en poder de los empresarios. Veamos: *"Considerando, sin embargo, que se precisan unas medidas que impidan la extracción y/o reutilización no autorizadas del contenido de una base de datos a falta de un régimen armonizado relativo a la competencia desleal o de la correspondiente jurisprudencia"*[132].

Aunado a ello, en las consideraciones se aprecian diversos motivos que condujeron a la expedición de esta Directiva, ente los que se destacan el reconocimiento del valor de los datos para el desarrollo del mercado comunitario, el reconocimiento del esfuerzo del fabricante de estas bases de datos y la necesidad de proteger el contenido. De esta forma, de manera expresa el considerando No. 45 señala que el derecho *sui generis* creado bajo esta Directiva puede entenderse como una ampliación a la protección otorgada por el Derecho de Autor, haciéndola extensiva a meros hechos o a los datos.

Tomando en cuenta los factores mencionados, entre otros, la Directiva a partir del capítulo III crea un derecho *sui generis* cuyo objeto de protección es el contenido de las bases de datos. En los términos del artículo 7, el objeto de protección de esta categoría jurídica es el siguiente:

> *"Los Estados miembros dispondrán que el fabricante de la base de datos pueda prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, cuando la obtención, verificación o presentación de dicho contenido representen una inversión sustancial desde el punto de vista cualitativo o cuantitativo".*

La figura supone, entonces, la posibilidad de que el fabricante de la base de datos o su derechohabiente -toda vez que se contempla la posibilidad de su transferencia, cesión o licenciamiento- prohíba o restrinja la explotación o reutilización total o parcial del contenido de la base de datos.

Posteriormente el mismo artículo añade que esta protección se entiende sin perjuicio de otros derechos que coexistan sobre la base de datos, como aquella del Derecho de Autor, o respecto de su contenido. En esa línea, el artículo 13 señala que el ejercicio de este derecho *sui generis* se entiende sin perjuicio de otras normas, entre las que se encuentran las relativas a la protección de datos personales. Desde esa perspectiva, en principio, no se encontraría colisión alguna entre los intereses del empresario y el titular de los datos.

Es claro que las disposiciones de la Directiva persiguen otorgar una protección en escenarios de competencia, es decir, ante las conductas de otros

132 Parlamento Europeo. Directiva 2016/943. (2016).

participantes del mercado, relativas a la sustracción o aprovechamiento de dicha información. Derivado de ello, resulta natural que se establezca un límite temporal a dicha prerrogativa, anticipándose a los efectos de mercado que dicha disposición pueda generar. En esa medida, el artículo 10 de la Directiva señala un plazo de protección de quince (15) años, empero, con el vencimiento de dicho plazo no podrá entenderse que tal contenido cae a dominio público, de manera analógica a lo que sucede en el régimen de Propiedad Intelectual. Ello como quiera que prevalezca las normas de orden público del régimen de protección de datos y que, adicionalmente, podría concurrir la protección por vía de secreto empresarial, en atención a lo analizado en el acápite anterior.

Se hace meritorio precisar que dicha Directiva es del año 1996, es decir que antecede veinte (20) años a la regulación actual en materia de protección de datos personales y secreto empresarial. Ello supone que esta regulación no se encuentra armonizada con las dinámicas actuales del mercado de datos e información, así como con las tendencias jurídicas en materia de protección de datos en el marco de la economía digital.

Actualmente, ante un escenario de globalización y mercados digitales mucho más sólido, los datos han cobrado un rol fundamental en la actividad empresarial, pero de una forma distinta a lo que podía pensarse hace veinte o treinta años. Gran parte de ello se debe al auge de otros desarrollos que acompañan la recolección, almacenamiento y análisis de datos, tales como las tecnologías de computación y almacenamiento en la nube. No obstante, la Directiva 96/9/CE ajustándose a los desarrollos tecnológicos de su época buscó regular la tenencia de los datos en poder del empresario como insumo de la actividad.

La Directiva 96/9/CE es un referente interesante de la protección de los datos personales como factor productivo, aun cuando puede encontrarse parcialmente desactualizado frente a las nuevas tendencias del mercado y al margen de que su aplicabilidad solo se ha considerado en territorio de la Unión Europea.

La creación de esta categoría de protección jurídica como un derecho *sui generis* se acompasa con las dificultades avizoradas en acápites anteriores, especialmente en punto a la naturaleza jurídica de los datos personales. Claramente, al tratarse de una figura especial no susceptible de ser ubicada en una disciplina preexistente del Derecho Comercial, su comprensión sigue siendo un reto, más allá de entender sus motivaciones y las prerrogativas que otorga.

Ahora bien, al margen del análisis de las categorías jurídicas propuestas, es imperativo referirnos al último eslabón de la cadena de valor de los datos, esto es, los datos analizados. Tal y como se evidenció mediante la entrevista No. 2, este es el estadio del que más provecho se obtiene de los datos, pues la información que contienen está depurada y estudiada, brindando para tal

efecto conclusiones que son ya el antecedente directo de la toma de decisiones gerenciales. Como tal, se trata de un producto independiente a los datos y las bases de datos, pues conlleva una intervención humana que los ha transformado.

De esta forma, estos pueden constituir incluso un programa de ordenador, el cual podrá ser protegido de manera independiente de conformidad con las normas de Propiedad Intelectual, sin perjuicio de otra forma que puedan adquirir y a los que sea atribuible la protección mediante otras disciplinas. Sin embargo, es de aclarar que en tales casos el objeto de protección es un producto independiente a los datos en sí mismos. Siendo que el estudio de las categorías de protección aplicables a los datos en esta etapa de la cadena de valor sobrepasa los límites propuestos para la investigación, solamente se dejan enunciados con el fin de brindar un panorama general de la vía de análisis a seguir.

Así entonces, la evaluación de las categorías jurídicas de protección aplicables a los datos personales tendrá que orientarse a la satisfacción del interés subyacente y, de esa forma, la valoración de las ventajas y retos que supone la aplicación de una categoría jurídica en concreto debe ser estudiada para cada caso en concreto.

A continuación se realizan unos breves apuntes conclusivos recogiendo los aspectos más relevantes de la investigación, de cara a brindar una perspectiva global de las posibles respuestas a la pregunta central de este escrito, así como poniendo de presente interrogantes que surgen de manera correlativa al abordaje que aquí se presentó.

4. CONCLUSIONES

El presente trabajo partió de una metodología de investigación socio-jurídica. Por ello, a pesar de que se busque brindar respuesta a un interrogante jurídico, se hacía imperativo entender la perspectiva técnica sobre los tipos de datos existentes en el entorno digital, así como la gerencial respecto del uso y aprovechamiento de los datos.

En punto a los tipos de datos personales y los datos en entornos digitales, una primera idea central y nuclear para el diseño regulatorio a futuro es que la noción de identificabilidad a que refieren las disposiciones que definen el dato personal puede encontrar más de un cuestionamiento tratándose de entornos digitales. Claro está que, aunque tal noción está dispuesta para los fines de la protección y garantía del derecho a la intimidad y privacidad de las personas, la virtualidad propia de los servicios digitales desdibuja esta identificabilidad y, por lo tanto, es válido cuestionarse sí metadatos, como aquellos que revelan preferencias de consumo, deberían -o no- ser considerados como un dato personal por asociación.

En un segundo término, el estudio de la perspectiva gerencial teórica y práctica, particularmente sobre el uso y aprovechamiento de los datos, ilustró con suficiente claridad distintos aspectos transcendentales para abordar la investigación y para vislumbrar los principales hitos a los que debe observar el regulador en el futuro.

El primero de estos aspectos fue comprender la magnitud de la utilidad e importancia de los datos para empresas de toda índole, mas no exclusivamente para empresas del sector tecnológico. En segundo lugar, a partir de las entrevistas practicadas se identificó que en la mayoría de casos el uso de estos datos está indefectiblemente ligado a otros desarrollos tecnológicos como la computación y almacenamiento en la nube, siendo esto una cuestión que cambia notablemente el escenario de los responsables del cumplimento normativo de protección de datos y sobre el interés del empresario en la protección de estos.

Para profundizar un poco más en este aspecto, conviene precisar que hoy en día las actividades relacionadas al aprovechamiento de datos comportan la necesidad de contar con sistemas tecnológicos que permitan su almacenamiento y procesamiento en masa. Si bien los costos asociados a tales procesos han disminuido con el advenimiento de nuevas tecnologías, la implementación de estos sistemas supone una carga importante para el empresario en términos económicos y logísticos. De ahí que el mercado haya migrado hacia la oferta particular e individualizada de estos servicios de almacenamiento y computación en la nube, como es el caso de Amazon Web Services, Azure o Google Cloud Platform, pues con la tercerización de estas actividades el empresario puede aprovechar sus datos, sin que ello suponga una mayor carga económica, logística y jurídica.

Nótese que mediante la entrevista No.1 se puso de presente que una forma utilizar los datos para la actividad empresarial es a través de la contratación de servicios finales ofrecidos por terceros. Servicios de *cloud computing* y *cloud storage* de Amazon Web Services, la analítica de datos que proporciona Google, el *target marketing* que ofrece Meta Platforms Inc., o el acceso a bases de datos de terceros como lo ofrece Microsoft a través de Linkedin Sales Navigator. Conviene entonces reconocer que existen múltiples modelos de gestión de los datos y de su aprovechamiento que escapan a los escenarios contemplados por la legislación vigente.

Retornando a los aspectos investigados de gran relevancia para responder al cuestionamiento central de este trabajo, desde la perspectiva jurídica y de política pública está el reconocimiento por parte del legislador de la existencia de un mercado de datos. Adicionalmente, se percibe que la postura generalizada es la de permitir el flujo de datos en el mercado interno y a nivel transfronterizo, con el balance necesario entre esta actividad económica y la protección a la privacidad de los titulares. Este es el primer peldaño para resolver el interrogante planteado. Pese a la connotación constitucional de

la protección de datos, no constituye un objeto ilícito su comercialización, siempre y cuando sea en cumplimiento de la normativa vigente para dar efectividad a los derechos fundamentales de los titulares. La comercialización y libertad en el flujo de datos es un escenario deseable. Lo anterior conlleva a reevaluar las posturas que buscan satanizar la recolección y tratamiento de datos con fines de la actividad empresarial.

Ahora bien, desde el estudio de las categorías jurídicas que servirían para la protección de los datos personales fue trascendental comprender que dicho análisis no puede, ni debe, hacerse de manera genérica. Como se vio, los datos en los diferentes estados de la cadena de valor constituyen un objeto distinto, por lo que las categorías jurídicas de protección susceptibles de ser evaluadas variarán en función del estado del dato.

Asimismo, un factor determinante en dicha valoración es el interés del empresario sobre el objeto de protección. Así como el interés de una empresa puede residir en la protección de esta en los estados más primigenios de la cadena de valor, también puede serlo la protección de un sistema de ordenador que se alimenta de tales datos, o para otra que le sea permitido contratar con terceros para obtener bienes o servicios derivados del uso de datos personales. Luego, desde la perspectiva jurídica subiste el cuestionamiento sobre cuál es el real objeto de protección tratándose de los datos personales como insumo de la actividad empresarial.

En el estudio de las categorías se hizo diáfano que no es posible de hablar de un Derecho Real de Dominio sobre los datos. A pesar de que desde la perspectiva económica pueda tener sentido que el empresario sea propietario de la *data* que recolecta y analiza, jurídicamente no es viable. Tampoco se encuentra una vía de protección efectiva por los medios de la propiedad industrial, como quiera que el concepto de patente -entre otros derechos de propiedad industrial- no encuadran con la naturaleza jurídica de los datos en cualquiera de sus estados dentro de la cadena de valor. Desde el Derecho de Autor la protección es limitada, como se anotó, la sola protección de la selección y disposición parece no ser suficiente para la protección de los datos como un factor productivo.

En contraste, la protección otorgada a partir del secreto empresarial se vislumbra más adecuada a los fines empresariales. Sin embargo, no se trata de una solución absoluta al ser necesaria su revisión caso a caso y al no encontrarse exenta de cuestionamientos, por ejemplo, en relación con la ambigüedad de ciertos conceptos, tales como el requisito de que esta información tenga valor. Por contera, el derecho *sui generis* que consagra la Directiva Europea 96/9/CE parece acertar en el objeto e intereses a salvaguardar, así como el tipo de protección que brinda, pero ¿Se acompasa dicha protección con las dinámicas actuales del mercado? Posiblemente no.

En todo caso, se aprecia desde la praxis que el empresario -independientemente del sector, actividad y tamaño de la empresa- no deja a la suerte el

acceso a sus datos. Por el contrario, se ha visto que el empresario detenta una tenencia de estos datos y, dependiendo de su actividad, favorece su acceso mediante la concesión de licencias, también conocidas como *end-user licence agreeements* (EULA), sin que ello suponga una contravención a lo dispuesto en las normas de protección de datos. Luego, pese a que desde el Derecho Positivo no se ha dispuesto de normas que busquen disciplinar el régimen de derecho privado aplicable a los datos personales como activo empresarial, las empresas han hecho uso de las categorías existentes para proteger sus intereses.

No existe una respuesta unívoca y absoluta frente al interrogante planteado en este escrito. La respuesta dependerá de un análisis individualizado del interés del empresario y, por esa vía, de la determinación del objeto de protección, a saber, el estado en que se encuentre la *data* en la cadena de valor. A juicio personal, no se hace necesario establecer una nueva categoría jurídica para su protección, aun cuando en el ordenamiento jurídico colombiano no se cuenta con una figura asimilable al derecho *sui generis* de la Directiva 96/9/CE. Seguramente por vía jurisprudencial se decanten algunos conceptos que permitan en el futuro tener una mayor claridad de la aplicabilidad de categorías jurídicas como el secreto empresarial. Esto, sin perjuicio de que el verdadero interrogante a propósito de los datos utilizados por los empresarios no verse sobre su propiedad, titularidad o tenencia, sino la protección de los datos personales de las personas jurídicas o, como se ha denotado en el derecho extranjero *corporate privacy* o *vie privée des affaires*.

Al margen de la resolución de esta inquietud, circundan a esta investigación otro tipo de interrogantes. En primer lugar, sigue siendo objeto de preocupación que las empresas transfieran datos personales de sus usuarios a diferentes gobiernos; dadas las inquietudes que suscita sobre prácticas de vigilancia estatal. De otra parte, una de las ideas que surge de la entrevista No. 1 es que gran parte de los datos recolectados, tratados, analizados y utilizados para ofrecer servicios finales son prestados por las grandes compañías como Google, Meta Platforms o Microsoft, por solo nombrar algunas[133]. Luego, no son pocos los cuestionamientos que surgen alrededor de los posibles efectos anticompetitivos que puedan derivarse de la tenencia y uso de datos por parte

133 Es preciso recordar que, de conformidad con la Ley de mercados digitales y aquella de Servicios Digitales de la Unión Europea, estas empresas -entre otras- pueden ser calificadas como gatekeepers o guardianes de acceso. Dada la omnipresencia y/o ubicuidad de estas empresas en distintos sectores, mercados e incluso mercados de precio cero, es alta la capacidad de estas para controlar varios aspectos del funcionamiento del mercado, más aún cuando son grandes recolectores de datos e información de usuarios a nivel global.

de estas empresas, así como dudas relacionadas con el cumplimiento de los estándares adecuados en materia de protección de datos[134].

Frente a este último punto, esto es, los efectos anticompetitivos que podrían derivar de la tenencia, uso y aprovechamiento de estas vastas cantidades de datos, la discusión sigue estando a la orden del día aun cuando las autoridades de protección a la libre competencia económica han hecho avances en esta dirección. Sobre este punto los análisis de las autoridades de competencia se han inclinado hacia la posibilidad de un abuso de la posición de dominio por la tenencia y uso de estos datos. Empero, la estructura de la normativa de protección a la libre competencia presenta grandes retos frente a la forma de dar aplicabilidad a ciertos conceptos que no funcionan propiamente en los mercados digitales, mercados multilaterales o mercados de precio cero, tales como el poder de mercado o los métodos de determinación del mercado relevante.

Por ejemplo, en el año 2019 la autoridad de competencia alemana (Bundeskartellamt) investigó a Facebook por políticas de recolección y tratamiento de datos personales abusivas, tanto en las páginas web Facebook.com, Facebook.de, aplicación móvil y otras aplicaciones externas asociadas al grupo empresarial, tales como Whatsapp, Masquerade o las aplicaciones para empresas[135]. Si bien la sanción se orientó a la protección de los datos personales, estableció aspectos interesantes para el Derecho de la Competencia, como la existencia de abuso de la posición dominante por vía de la implementación de la política de datos personales de Facebook. Veamos:

> *"El uso e implementación efectiva de la política de datos de Facebook, que permite a la plataforma recopilar datos de usuarios y dispositivos desde fuentes externas a la red social y fusionarlos con datos recolectados en Facebook, constituye un abuso de una posición dominante en el mercado de redes sociales en forma de términos comerciales explotativos según la cláusula general de la Sección 19(1) GWB. Teniendo en cuenta las evaluaciones en materia de protección de datos conforme al Reglamento General de Protección de Datos (RGPD), estos términos son inapropiados y perjudiciales tanto para los usuarios privados como para los competidores"*[136].

134 Como referencia de este asunto, recientemente el Comité Europeo para la Protección de Datos sancionó a Meta Platforms Inc por la transferencia de datos de ciudadanos europeos a Estados Unidos, sin el cumplimiento de los estándares y niveles de protección requeridos. Para el efecto remitirse a: https://www.dw.com/en/eu-fines-meta-12-billion-over-data-transfers-to-us/a-65695990#:~:text=European%20Union%20regulators%20on%20Monday,a%20previous%20EU%20court%20ruling.

135 Bundeskartellamt. Case summary B6-22/16. (2019). https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=#:~:text=Using%20and%20actually%20implementing%20Facebook's,form%20of%20exploitative%20business%20terms

136 Ibíd.

De otra parte, el pasado 14 de junio de 2023, la Comisión Europea decidió investigar de manera formal a Google Inc. por presunto abuso de la posición dominante en los mercados de publicidad digital[137], como quiera que presuntamente habría tendido a favorecer a sus propios bienes o servicios en sus plataformas de servicios de publicidad[138]. Lo anterior encuentra un matiz interesante, por cuanto se trata de servicios que Google Inc. ofrece con base en los datos que recolecta a partir de sus servicios gratuitos, tales como los motores de búsqueda. Sobre este punto señaló Magrethe Vestager vicepresidenta ejecutiva a cargo de la política de competencia:

> *"Google tiene una posición muy sólida en el sector de la tecnología publicitaria en línea. Recopila datos de usuarios, vende espacios publicitarios y actúa como intermediario en la publicidad en línea. Por lo tanto, Google está presente en casi todos los niveles de la llamada cadena de suministro de la tecnología publicitaria. Nuestra preocupación preliminar es que Google podría haber utilizado su posición en el mercado para favorecer sus propios servicios de intermediación. Esto no solo podría haber perjudicado a los competidores de Google, sino también a los intereses de los editores, al tiempo que aumentaba los costos de los anunciantes. Si se confirma, las prácticas de Google serían ilegales según nuestras reglas de competencia"*[139].

Como se aprecia, particularmente en el campo de la política de protección a la libre competencia económica, así como en materia de Propiedad Intelectual y Protección al Consumidor, son muchos los cuestionamientos que surgen y seguirán originándose en relación con los datos personales utilizados para la actividad empresarial. Luego, estos son asuntos que seguirán siendo objeto de discusión y estudio en el futuro. Los aspectos asociados con los datos personales, dado el auge en su uso y su relevancia para las economías digitales, siguen siendo puntos en constante evolución a los que el derecho debe responder de manera articulada y armónica con las dinámicas y tendencias del mercado, así como a la perspectiva de la política pública para satisfacer de manera balanceada los intereses del conglomerado social.

137 En particular se hace referencia a los siguientes mercados: i) el mercado para servidores de anuncios de editores con su servicio 'DFP'; y (ii) para herramientas de compra programática de publicidad para la web abierta con sus servicios 'Google Ads' y 'DV360. Comisión Europea. Conferencia de prensa de 14 de junio de 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP _23_3207

138 Comisión Europea. Conferencia de prensa de 14 de junio de 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP _23_3207

139 Ibíd.

REFERENCIAS

Legales

Carta de Derechos Fundamentales de la Unión Europea, (2000). https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Congreso de la República de Colombia. (20 de julio de 1991). Constitución Política de Colombia. Gaceta Constitucional 116.

Congreso de la República de Colombia. (17 de Octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. [1581 de 2012]. DO: [48.587].

Congreso de la República de Colombia. (31 de diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Ley 1266 de 2008]: DO: [47.219]

Congreso de la República de Colombia. (2010). *Gaceta No. 1.023*.

Congreso de la República de Colombia. (31 de Diciembre 31 de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [1266 de 2008]. DO: [47.219].

Convención Europea de Derechos Humanos, (1950).

Consejo de Europa. (1981). Convenio 108.

Consejo de Europa. (2018). Convenio 108+.

Ministerio de Industria, Comercio y Turismo. (27 de junio de 2013). Por la cual se reglamenta parcialmente la Ley 1581 de 2012.

Parlamento Europeo. (2016). Directiva 2016/943,

Parlamento Europeo. (1996). Directiva 96/9/CE.

Parlamento Europeo. (2002). Directiva 2002/58 CE.

Parlamento Europeo. Reglamento 2016/679: Reglamento General de Protección de Datos , (2016). https://www.boe.es/doue/2016/119/L00001-00088.pdf

Parlamento Europeo. Reglamento 2018/1807: Relativo a un marco para la circulación de datos no personales en la Unión Europea, ReglamentoU.S.C. (2018). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1807&from=ES

Tratado de Funcionamiento de la Unión Europea (TFUE), (2012).

Jurisprudenciales

Bundeskartellamt. Case summary B6-22/16. (2019). https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=#:~:text=Using%20and%20actually%20implementing%20Facebook's,form%20of%20exploitative%20business%20terms

Comisión Europea. Conferencia de prensa de 14 de junio de 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP _23_3207

Digital rights Ireland Ltd & Seitlinger y otros, Tribunal de Justicia de la Unión Europea. (2014). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293&from=es

Doctrinales

Ahmed, E., Yaqoob, I., Hashem, I. A. T., Khan, I., Ahmed, A. I. A., Imran, M., & Vasilakos, A. V. (2017). The role of big data analytics in Internet of Things. *Computer Networks*, *129*. https://doi.org/10.1016/j.comnet.2017.06.013

Banerjee, S. (Sy), Hemphill, T., & Longstreet, P. (2018). Wearable devices and healthcare: Data sharing and privacy. *Information Society*, *34*(1). https://doi.org/10.1080/01972243.2017.1391912

Bargmeyer, B. E., & Gillman, D. W. (2000). Metadata standards and Metadata registries: an overview. *Vasa*.

Bender, D., & Ponemon, L. (2006). Binding corporate rules for cross-border data transfer. *Rutgers JL & Urb.Pol'Y*, *3*, 154.

Briones Delgado, J. M. (2014). *Datos, información y conocimiento: promesas y realidades de la red global*

Bodie, M. T., Cherry, M. A., McCormick, M. L., & Tang, J. (2017). The Law and Policy of People Analytics. *University of COlorado Law Review*, *88*(4).

Carrascal, J. P., Riederer, C., Erramilli, V., Cherubini, M., & De Oliveira, R. (2013). Your browsing behavior for a big mac: Economics of personal information

online. Paper presented at the *Proceedings of the 22nd International Conference on World Wide Web*, 189-200.

Carrière- Swallow, Y., & Haksar, V. (2019). *The Economics and Implications of Data: An Integrated Perspective*. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/20/The-Economics-and-Implications-of-Data-An-Integrated-Perspective-48596

Castellanos Pfeiffer, R. A. (2019). Digital economy, big data and competition law. *Mkt.& Competition L.Rev.*, *3*, 53.

Conseil National du Numérique. (2017). *La libre circularion des donneés dans L'Union Européenne*

Consejo Nacional de Política Económica y Social, Departamento Nacional de Planación. (2018). *Documento CONPES 3920*. (). Bogotá, Colombia:

De Mauro, A., Greco, M., & Grimaldi, M. (2015). What is big data? A consensual definition and a review of key research topics. Paper presented at the *AIP Conference Proceedings*, *1644*(1) 97-104.

DeSimone, C. (2010). Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive. *German Law Journal*, *11*(3), 291-317. 10.1017/S2071832200018538

Domdouzis, K., Lake, P., & Crowther, P. (2021). Data, An Organisational Asset. In K. Domdouzis, P. Lake & P. Crowther (Eds.), *Concise Guide to Databases: A Practical Introduction* (pp. 3-21). Springer International Publishing. 10.1007/978-3-030-42224-0_1

Faroukhi, A. Z., El Alaoui, I., Gahi, Y., & Amine, A. (2020). Big data monetization throughout Big Data Value Chain: a comprehensive review. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-019-0281-5

Ferreira Mendes, L. S. (2018). Information Self-Determination and Habeas Data: Two Sides of the Same Coin? *Direitos Fundamentais & Justica*, *39*, 185-216. http://basesbiblioteca.uexternado.edu.co:2048/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=edshol&AN=edshol.hein.journals.direfnj39.10&lang=es&site=eds-live&scope=site.

Foro Económico Mundial, & Bain & Company Inc. (2011). Personal data : The emergence of a new asset class.

Gates, C., & Matthews, P. (2014). Data is the new currency. Paper presented at the *Proceedings of the 2014 New Security Paradigms Workshop*, 105-116.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. In Computers and Security (Vol. 77). https://doi.org/10.1016/j.cose.2018.04.002

González Guerrero, L. D. (2019). Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. *Estudios Socio-Jurídicos*, *21*(1), 209-244.

Google, L. (2022). *Página de ayuda de Google Chrome*. https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=es#:~:text=Las%20cookies%20son%20archivos%20que,contenido%20relevante%20seg%C3%BAn%20tu%20ubicaci%C3%B3n

Guadamuz, A. (2001). Habeas Data vs the European Data Protection Directive. *The Journal of Information, Law and Technology,* The Journal of Information, Law and Technology

Grupo de acceso a la información y protección de datos personales. (n.d.). Protección de datos personales. Registraduría Nacional del Estado Civil .

Haller, S., Karnouskos, S., & Schroth, C. (2009). The Internet of things in an enterprise context. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5468. https://doi.org/10.1007/978-3-642-00985-3_2

Hjørland, B. (2018). Data (with Big Data and Database Semantics). *Official Journal of the International Society for Knowledge Organization*, (8)

Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. Computer Law & Security Review, 25(1), 84–88. https://doi.org/https://basesbiblioteca.uexternado.edu.co:2199/10.1016/j.clsr.2008.11.002

Janeček, V. (2018). Ownership of personal data in the Internet of Things. Computer Law and Security Review, 34(5). https://doi.org/10.1016/j.clsr.2018.04.007

Jarman, S., & Örsal, D. D. K. (2020). The regulation of zero-price markets by the competition authorities in the USA and the EU. *Competition and Regulation in Network Industries*, *21*(4), 315-343.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134.

Korff, D., & Georges, M. (2020). *The Origins and Meaning of Data Protection*

KPMG. (2019). *Data as an asset*

Kristol, D. M. (2001). HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology (TOIT), 1*(2), 151-198.

Llaneza González, P. (2019). *Datanomics: todos los datos personales que das sin darte cuenta y todo lo que las empresas hacen con ellos*. Editorial Planeta Colombiana, Editorial Planeta, Ediciones Paidós.

Machlup, F., & Mansfield, U. (1983). *The Study of Information (Interdisciplinary Messages)*. Willey.

Marr, B. (2018). *Data strategy: cómo beneficiarse de un mundo de Big Data, analytics e internet de las cosas*. Ecoe Ediciones.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data: the management revolution. *Harvard Business Review, 90*(10), 60-68.

OECD. (2013). *Exploring the Economics of Personal Data: A survey of methodologies for measuring monetary value*. ().https://doi.org/https://doi.org/10.1787/5k486qtxldmq-en https://www.oecd-ilibrary.org/content/paper/5k486qtxldmq-en

OECD. (2015). *Data-Driven* Innovationhttps://doi.org/https://doi.org/10.1787/9789264229358-en

Pérez Luño, A. E. (1992). Del habeas corpus al habeas data. *Informática Y Derecho: Revista Iberoamericana De Derecho Informático*, (1), 153-161.

Perrons, R. K., & Jensen, J. W. (2015). Data as an asset: What the oil and gas sector can learn from other industries about "Big Data". *Energy Policy, 81*, 117-121.

Polo Roca, A. (2021). *Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos*. University of Deusto. 10.18543/ed-69(1)-2021pp211-240

Puyol Moreno, J. (2014). Una aproximación a Big Data. Revista de Derecho de La UNED (RDUNED), 14. https://doi.org/10.5944/rduned.14.2014.13303

Sanchez-Rola, I., Ugarte-Pedrero, X., Santos, I., & Bringas, P. G. (2017). The web is watching you: A comprehensive review of web-tracking techniques and countermeasures. *Logic Journal of the IGPL, 25*(1), 18-29.

Schneier, B. (2018). Data and Goliath : the hidden battles to collect your data and control your world.

Solove, D. J. (2021). The Myth of the Privacy Paradox. George Washington Law Review, 89(1). https://doi.org/10.2139/ssrn.3536265

Stengel, D. (2004). La propiedad intelectual en la filosofía. Revista La Propiedad Inmaterial , 8, 71–106.

Stucke, M. E. (2022). What Are the Policy Implications if Data Is Non-rivalrous? In M. E. Stucke (Ed.), *Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy* (pp. 0). Oxford University Press. 10.1093/oso/9780197617601.003.0007

Stucke, M., & Grunes, A. (2016). Part I The Growing Data-Driven Economy, 2 Defining Big Data . *Big Data and Competition Policy* (Oxford Competition Law ed.,)

Véliz, C. (2022). Privacy Is Power: Why and How You Should Take Back Control of Your Data. In International Data Privacy Law (Issue 3). https://doi.org/10.1093/idpl/ipac007

Von Dietze, A., & Irvine-Geddis, J. (2019). *Data as an Asset*.