



**PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE CIENCIAS JURÍDICAS**

DEPARTAMENTO DE DERECHO ECONÓMICO

**Reglamento General de Protección de Datos de la Unión Europea:
Limitaciones a los sistemas de toma de decisiones automatizados, ineficiencia en los
mercados de datos y restricciones a la libre competencia económica.**

SANTIAGO BLANCO ANGULO

DIRECTOR: VÍCTOR AYALDE LEMOS

**BOGOTÁ D.C.
2019**

Tabla de Contenido

1. Resumen.....	4
2. Introducción	5
i) Planteamiento del problema	5
ii) Antecedentes en el tratamiento automatizado de datos personales	6
iii) Antecedentes normativos en la protección de datos e influencia de la experiencia alemana	11
iv) Noción de datos personales como un mercado	18
3. Reglamento General de Protección de Datos de la Unión Europea.....	21
i) Antecedentes y fundamentos para la adopción de la Regulación	21
a. Reemplazo de la Directiva de Protección de Datos de 1995	22
b. Fundamento en los Considerandos	24
ii) Generalidades sobre el nuevo Reglamento	25
iii) Artículo 22	35
a. Decisiones automatizadas individuales.....	37
b. <i>Profiling</i>	38
c. Noción de “ <i>decisiones que produzcan efectos jurídicos</i> ” o “ <i>que afecten significativamente o de modo similar</i> ” al interesado.....	42
d. Excepciones a la restricción.....	44
e. Dificultades interpretativas del artículo 22	45
4. Procesos automatizados de toma de decisiones y <i>profiling</i>	50
i) Usos prácticos en la actualidad y posibles usos en el futuro	50
ii) Ventajas de usar sistemas automatizados de toma de decisiones en el tratamiento de Big Data	56

iii)	Efectos del Artículo 22 en materia de libre competencia económica...	58
a.	Posibles desincentivos para la innovación en nuevas tecnologías..	59
b.	Barreras de entrada al mercado.....	64
c.	Mayor concentración en el mercado de datos.....	71
5.	Toma de decisiones automatizadas y el argumento de la discriminación	78
6.	Conclusiones.....	83
i)	Conclusión respecto del análisis histórico en el tratamiento automatizado de datos y antecedentes históricos en materia de normas sobre datos personales.....	84
ii)	Conclusión respecto de los principales elementos que introduce el Reglamento General de Protección de Datos de la Unión Europea.....	84
iii)	Conclusión respecto de los procesos automatizados de toma de decisiones y <i>profiling</i>	85
iv)	Conclusión respecto de los efectos que el artículo 22 del Reglamento General de Protección de Datos tiene sobre la libre competencia económica y respecto del argumento de la discriminación	86
v)	Respuesta a la pregunta de investigación.....	88
7.	Bibliografía	89

1. Resumen

En 2018 la Unión Europea implementó el Reglamento General de Protección de Datos, norma que restringe el uso de sistemas tomas de decisiones automatizadas a partir del tratamiento de datos personales, cuando dichas decisiones tengan efectos jurídicos o afecten de manera similar a los interesados. El presente trabajo de grado consiste en una reflexión sobre si el nuevo Reglamento General de Protección de Datos de la Unión Europea resulta perjudicial para los mercados de datos y el desarrollo de nuevas tecnologías, o si se trata de una medida justificable en pro de la protección de información personal de individuos.

***Palabras clave:** Tratamiento automatizado, profiling, limitaciones, datos personales.*

2. Introducción

i) Planteamiento del problema

El presente trabajo de investigación se enfocará principalmente en las restricciones impuestas en los agentes del mercado, a raíz de la entrada en vigencia del Reglamento General de Protección de Datos Personales de la Unión Europea. Su finalidad será determinar si a partir de esta nueva legislación se generan ineficiencias en el mercado de datos que resulten nocivas para las industrias emergentes y la libre competencia económica, o si, por otro lado, se trata de una medida justificable en pro de la información personal de los individuos. En este sentido, se plantea la siguiente pregunta de investigación:

¿Es el Reglamento General de Protección de Datos de la Unión Europea un desincentivo para el desarrollo de los mercados de datos y la libre competencia económica?

Con el fin de introducir el presente trabajo de investigación, en seguida se hará un breve recuento de algunos de los principales avances tecnológicos en materia de sistemas de tratamiento de datos personales, principalmente en Europa, abarcando etapas relevantes desde las máquinas tabuladoras del siglo XIX hasta el surgimiento de la World Wide Web. Posteriormente, se hará una breve mención de algunas de las primeras legislaciones europeas en materia de protección de datos personales, haciendo especial énfasis en la experiencia histórica alemana, proponiéndola como un factor determinante en el surgimiento de la política europea de tratamiento de datos personales vigente, política que se ve plasmada en el Reglamento General de Protección de Datos. Para finalizar, se planteará la noción del mercado

de datos personales teniendo en cuenta algunos conceptos desarrollados por la Comisión Europea, los cuales serán tenidos en cuenta a lo largo del trabajo de investigación.

ii) Antecedentes en el tratamiento automatizado de datos personales

En esta sección, se estudiará la forma en que a lo largo de la historia reciente se empezaron a sistematizar la recolección y tratamiento de datos en general, dentro de los cuales se incluyen los datos personales. Lo anterior, como fruto de diferentes avances tecnológicos que permitieron el tratamiento de manera más ágil, por métodos que permitían variaciones a la simple recolección y organización manual de datos. De esta forma, se explicará cómo se implementaron sistemas de tratamiento automatizado con fines estadísticos en Estados Unidos, y su eventual adopción en Europa. Posteriormente, se explicará cómo el uso que se les dio en Alemania tuvo consecuencias negativas, y cómo éstos serían usados para fines militares durante la Segunda Guerra Mundial. En seguida, se hará mención sobre la forma en que se les empezó a dar un uso comercial y cómo el público en general empezó a tener acceso a estos sistemas para su uso diario. Para finalizar, se hará un breve recuento del surgimiento de la World Wide Web.

A finales del siglo XIX, en Estados Unidos se empezaron a desarrollar diferentes metodologías para la recolección de datos. En principio, la recolección tenía como objetivo la obtención de datos estadísticos con el fin de hacer estudios de censo.¹ Para el Gobierno Federal, realizar dichos estudios era necesario para cumplir con un mandato constitucional en el que se le ordena realizar un censo poblacional cada 10 años.² Debido al crecimiento en la población y la

¹ Jim Gray, "Evolution of Data Management", *Computer*, 29 no. 10 (1996): 40, <https://pdfs.semanticscholar.org/ba69/4ef52cda8f666d9a0e0aabf2135b7d1b3f7a.pdf>

² Constitución de los Estados Unidos. Artículo 1, Sección 2.

diversidad de información que era requerida de cada persona, con los métodos de tabulación de la época, los censos podían tardar varios años en publicar sus resultados.³ Así, se llegó a calcular que para el censo de 1890, el Gobierno tardaría más de 10 años en publicar la información.⁴

Lo anterior llevó a que por primera vez se usara la maquina tabuladora Hollerith, desarrollada por el ingeniero Herman Hollerith, para el censo de 1890.⁵ La misma proveía un sistema más rápido y organizado para procesar la información a través de tarjetas perforadas o “*punchcards*”. Este permitía organizar la información recaudada en agujeros perforados en las tarjetas, las cuales eran después introducidas en un lector mecánico que almacenaba dicha información. Cada agujero representaba información diferente recolectada sobre las personas censadas, permitiendo así que el tratamiento de información no superara los tres años, ahorrando al gobierno una suma cercana a cinco millones de dólares de la época.⁶

El sistema fue introducido en Europa en años siguientes para los censos en Austria, Francia, Noruega, y Rusia.⁷ En aquel tiempo, Hollerith fundó la Tabulating Machine Company, empresa que después se fusionaría con otras compañías para crear la Computing Tabulating Recording Company en 1911, que en 1924 cambiaría su nombre a International Business Machines Corporation, conocida actualmente por su nombre comercial como IBM.⁸

³ Departamento de Comercio de los Estados Unidos, Oficina del Censo, División de Datos de Usuarios, “*100 Years of Data Processing*”, enero de 1991, 4, <https://play.google.com/books/reader?id=uCeu4sHRLfgC&hl=en&pg=GBS.PA4>

⁴ *Ibidem*, 5.

⁵ Frank da Cruz, “*Herman Hollerith*”, Columbia University, última actualización 30 de mayo de 2019, <http://www.columbia.edu/cu/computinghistory/hollerith.html>

⁶ Joseph Stromberg, “*Herman Hollerith’s Tabulating Machine*”, Smithsonian, 9 de diciembre de 2011, <https://www.smithsonianmag.com/smithsonian-institution/herman-holleriths-tabulating-machine-2504989/>

⁷ “*Tabulating Machine*”, History-Computer, no hay fecha, https://history-computer.com/ModernComputer/Basis/TabulatingMachine_Hollerith.html

⁸ Frank da Cruz, “*Herman Hollerith*”, Columbia University, última actualización 30 de mayo de 2019, <http://www.columbia.edu/cu/computinghistory/hollerith.html>

El tratamiento de datos personales entre 1890 y 1940 fue llevado a cabo principalmente por variaciones del mismo sistema de perforación de tarjetas, tanto para efectos del tratamiento de datos demográficos, como para otros tipos de información. Estos avances se convirtieron en una necesidad para que los Estados pudiesen llevar a cabo tareas que requerían del manejo de grandes cantidades de información sobre sus ciudadanos.⁹

Pese a su gran utilidad como medio de tratamiento y análisis de información demográfica, el uso de estos primeros sistemas también ha sido fuente de controversia. En Alemania durante la década de 1930, las máquinas de Holerith también eran usadas con el fin de procesar información estadística de la población.¹⁰ Agentes del censo acudían a los hogares de las personas cargando tarjetas para perforación con el fin de obtener información de los ciudadanos, procesarla y almacenarla. Hay quienes argumentan que dicha información estadística sería la misma empleada durante el holocausto como una forma de identificar personas que serían enviadas a campos de concentración.¹¹

La forma en la que se recolectaban y trataban los datos fue evolucionando a lo largo del tiempo. Durante la Segunda Guerra mundial se desarrollaron sistemas que recolectaban y descifraban grandes cantidades de información. Parte importante de la estrategia militar de los aliados fue el desarrollo del Colossus Mark I en Inglaterra y el ENIAC en Estados Unidos.¹² Es necesario mencionar ambos sistemas debido a que han sido considerados como uno de los primeros

⁹ Jim Gray, “*Evolution of Data Management*”, *Computer*, 29 no. 10 (1996): 40, <https://pdfs.semanticscholar.org/ba69/4ef52cda8f666d9a0e0aabf2135b7d1b3f7a.pdf>

¹⁰ Olivia Waxman, “*The GDPR in Just the Latest Example of Europe’s Caution on Privacy Rights. That Outlook Has a Disturbing History*”, *Time Magazine*, mayo 24 de 2018, <http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>

¹¹ Edwin Black, “*IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America’s Most Powerful Corporation*”, (No hay ciudad: Crown Books, 2001.)

¹² “*Birth of Colossus and Enniac*”, It History, no hay fecha, http://it-history.net/colossus_and_ENIAC.html

computadores digitales en el mundo.¹³ El principal uso del Colossus Mark I, diseñado en marzo de 1943, era el de descifrar mensajes encriptados alemanes. Su procesamiento lógico era llevado a cabo principalmente a partir de tubos al vacío, grabando la información recuperada en cinta perforada que representaba los mensajes interceptados.¹⁴ Su principal función era descifrar los mensajes en código que salían de la máquina de cifrado alemana Lorenz SZ-40/42, emitidos por el alto comando alemán.¹⁵

ENIAC fue construido en la Universidad de Pensilvania durante la guerra y presentado al público en 1946.¹⁶ Al igual que el Colossus Mark I, usaba sistemas lógicos a base de tubos al vacío, y aunque fue diseñado originalmente para realizar mediciones de rondas de artillería para el ejército estadounidense,¹⁷ la guerra terminó antes de que pudiese operar de manera plena, por lo que sus uso militar cambió, y fue reprogramado para resolver problemas relacionados con en el desarrollo de la bomba de hidrógeno.¹⁸ Al igual que el Colossus, durante esta etapa, la naturaleza de la información recogida no estaba realmente relacionada con datos personales, sino con mensajes cifrados, estadísticas y mediciones para uso militar.¹⁹ Sin embargo, sin estos no se podrían haber desarrollado computadores de primera generación en décadas posteriores, ni se habría generado un impacto en la opinión pública sobre el uso de este tipo de sistemas.²⁰

¹³ Ibid.

¹⁴ “*The Colossus Machine*”, Stanford Computer Science, no hay fecha, <https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/colossus.html>

¹⁵ “*Colossus Birth of the Digital Computer*”, Crypto Museum, no hay fecha, <https://www.cryptomuseum.com/crypto/colossus/index.htm>

¹⁶ Paul Atkinson, “*ENIAC versus Colossus and the early presentation of electronic computers*”, Universidad de Oxford, 2014, 5, http://shura.shu.ac.uk/9501/3/Atkinson_-_Eniac_versus_Colossus_paper_%26_url.pdf

¹⁷ Ibid., 3

¹⁸ “*ENIAC*”, Engeniering and Technology, última actualización el 23 de noviembre de 2017, <https://ethw.org/ENIAC>

¹⁹ Ibid.

²⁰ Paul Atkinson, “*ENIAC versus Colossus and the early presentation of electronic computers*”, Universidad de Oxford, 2014, 5, http://shura.shu.ac.uk/9501/3/Atkinson_-_Eniac_versus_Colossus_paper_%26_url.pdf

A inicios de la década de 1950, fue desarrollado el Lyons Electronic Office (LEO) en Inglaterra.²¹ Se trató de un sistema que podía manejar toda clase de información contable de carácter empresarial, incluyendo información relativa a clientes, empleados, e información salarial, procesando la información recolectada a una velocidad de 500MHz por segundo.²² Es importante hacer mención del LEO debido a que permitió que no fuese solo el Estado, sino también las compañías privadas las que tuviesen acceso a estos sistemas para el manejo de datos sobre personas naturales.

Durante las décadas de 1970 y 1980, fueron importantes la comercialización masiva del computador personal y el desarrollo del microprocesador.²³ Lo anterior permitió una significativa reducción en tamaño y costo de los computadores, que a su vez tuvo como efecto que no fuesen sólo entidades gubernamentales y grandes compañías quienes tuviesen acceso a dichos sistemas, sino que los mismos estuviesen disponibles para el público en general.²⁴

En los años siguientes, Timothy Berners Lee, ingeniero de software de la Universidad de Oxford, identificó que era muy difícil compartir información entre los diferentes computadores del Centro de Investigación de Energía Nuclear Europeo (CERN).²⁵ En 1989, previó que era posible hacer uso de una tecnología emergente denominada “hipertexto” para desarrollar un nuevo sistema de comunicación que eventualmente sería conocido como la World Wide Web.²⁶ El 30 de abril de 1993 CERN anunció que la World Wide Web sería de uso público,

²¹Tom Jowitt, “*World’s First Business Computer, LEO, Turns 60*”, Silicon, noviembre 11 de 2011, https://www.silicon.co.uk/workspace/worlds-first-business-computer-leo-turns-60-45618?inf_by=5c1991e3671db8176e8b4577

²²Ibid.

²³Graham Singer, “*History of the Microprocessor and the Personal Computer, Part 2*”, septiembre de 2014, <https://www.techspot.com/article/884-history-of-the-personal-computer-part-2/>

²⁴Ibid.

²⁵David Grossman, “*On this Day 25 years ago, the Web Became Public Domain*”, Popular mechanics, abril de 2018, <https://www.popularmechanics.com/culture/web/a20104417/www-public-domain/>

²⁶“*History of the Web*”, World Wide Web Foundation, no hay fecha, <https://webfoundation.org/about/vision/history-of-the-web/>

permitiendo acceso a esta desde cualquier computador con una conexión activa a nivel mundial.²⁷ Es necesario hacer mención de esta etapa debido a que la disponibilidad de información y el libre acceso a internet sería el primer paso para el surgimiento de nuevos mercados en los cuales se transarían no solo bienes y servicios, sino todo tipo de datos, como será explicado más adelante.

Habiendo mencionado algunos de los principales desarrollos técnicos en el tratamiento de datos personales, a continuación, se examinarán algunos de los principales desarrollos normativos en materia de regulación de protección de datos en Europa.

iii) Antecedentes normativos en la protección de datos e influencia de la experiencia alemana

En esta sección, se mencionarán algunos antecedentes normativos en materia de privacidad y protección de datos personales en Europa. Posteriormente, se explicará cómo algunos antecedentes de la historia alemana fueron un factor que influyó en la adopción de la política de protección de datos vigente en Europa. Para ello, se hará énfasis en la vigilancia de ciudadanos durante los regímenes de la Alemania Nazi y de la República Democrática Alemana, así como su impacto en la Decisión del Tribunal Constitucional Alemán del 15 de diciembre de 1983. La experiencia alemana resulta relevante para el presente trabajo de investigación debido a que ayuda a explicar por qué la legislación europea vigente es una de las más estrictas en materia de protección de datos.

²⁷ David Grossman, “*On this Day 25 years ago, the Web Became Public Domain*”, Popular mechanics, abril de 2018, <http://radar.oreilly.com/2012/03/data-markets-survey.html>

Primero, cabe resaltar que la Declaración Universal de los Derechos Humanos es un antecedente importante en cuanto a la protección de datos en Europa. El artículo 12 de la Declaración consagra el derecho a la privacidad en la siguiente forma;

*“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.”*²⁸

Igualmente, la Convención Europea de los Derechos Humanos de 1950 consagra el derecho al respeto de la vida privada y familiar. El artículo 8 de la Convención establece;

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

*2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto 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.”*²⁹

²⁸ Asamblea General de las Naciones Unidas, Declaración Universal de los Derechos Humanos, diciembre 10 de 1948, artículo 12, <https://www.un.org/es/universal-declaration-human-rights/>

²⁹ Consejo de Europa, Convención Europea de Derechos Humanos, 3 de septiembre de 1953, artículo 8, https://www.echr.coe.int/Documents/Convention_SPA.pdf

En los años siguientes al reconocimiento de estos derechos, distintos países en Europa comenzaron a redactar leyes que buscaban proteger el derecho a la privacidad de sus ciudadanos de manera más concreta. En 1970 se expidió la Ley de Protección de Datos del Estado de Hesse en Alemania (*Hessisches Datenschutzgesetz*), la cual ha sido reconocida como la primera ley de protección de datos en el mundo.³⁰ Esta fue reemplazada en 1977 por la Ley Federal de Protección de Datos (*Bundesdatenschutzgesetz*), la cual ampliaba la regulación de protección de datos a nivel nacional.³¹ Posterior a la Ley Federal del Estado de Hesse, Suecia adoptó la Ley de Protección de Datos de 1973 (*Datalagen*),³² en Francia fue adoptada la Ley 78-17 de Protección de Datos de 1978 (*Loi 78-17*),³³ y en el Reino Unido la Ley de Protección de Datos de 1984 (*Data Protection Act*).³⁴

Es importante hacer mención del fallo del Tribunal Constitucional Federal Alemán respecto del Censo Poblacional de 1983.³⁵ En aquel año, fueron recibidas múltiples quejas por violaciones de derechos constitucionales a raíz de un censo que planeaba realizar el Gobierno Alemán.³⁶ El nivel de inconformidad que este generó, llevó a que el mismo fuese demandado ante el Tribunal Constitucional en aquel año.³⁷ Recibida la demanda, y después de un extenso análisis del acto demandado, el Tribunal encontró que éste era parcialmente inconstitucional

³⁰ Andrew Charlesworth, "A Very Short History of Data Protection", Cloud View, no hay fecha, <http://www.cloudview.co/Averyshorthistoryofdataprotection> : "The first rudimentary DP law is widely recognised to be that of Hesse, Germany in 1970."

³¹Parlamento Federal Alemán, Ley Federal de Protección de Datos, enero 27 de 1977, https://www.bgbl.de/xaver/bgbl/media/DD5B0A8907DA04DC249329E46ACA760B/bgbl177i0201_39307.pdf

³² Asamblea Legislativa del Reino de Suecia, Ley de Datos, mayo 11 de 1978, <http://rkrattsbaser.gov.se/sfst?bet=1973:289>

³³ Asamblea Nacional de Francia, Ley 78-17 sobre datos, archivos y libertades, enero 6 de 1978, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>

³⁴ Parlamento del Reino Unido, Ley de Protección de Datos, julio 12 de 1984, http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf

³⁵ Tribunal Constitucional Alemán, Sentencia del 15 de diciembre de 1983, BVerfGE 65,1 – Censo, diciembre 15 de 1983, versión traducida al inglés, <http://www.servat.unibe.ch/dfr/bv065001.html>

³⁶ Gerrit Hornung, Christoph Schnabel, "Data Protection in Germany I: The Population Census Decision and the right to information and self-determination", *Computer Law and Security Report*, Universidad de Kessel, Alemania, 25 no. 1, (229): 4, <https://doi.org/10.1016/j.clsr.2008.11.002>

³⁷ Ibid.

debido a su incompatibilidad con los artículos 2 (1) y 1(1) de la Ley Fundamental de la República Federal Alemana.³⁸ La decisión tuvo como efecto el reconocimiento de un derecho a la “autodeterminación informativa” (*informationelle Selbstbestimmung*).³⁹

Para el Tribunal, el reconocimiento de este derecho implicaba una garantía para todo individuo de tomar decisiones respecto de la posibilidad de que su información fuese revelada o divulgada.⁴⁰ Mediante esta decisión, se ordenó por primera vez al gobierno adoptar medidas para garantizar la confidencialidad de la información compartida por los censados.⁴¹ Es importante resaltar que los derechos a la privacidad y a la autodeterminación informativa no están explícitamente consagrados en la Ley Fundamental.⁴² Sin embargo, a raíz de una consideración conjunta del derecho a la dignidad humana (Art. (2) (1)) y del derecho a la libertad personal (Art. (2) (1), que conforman el derecho de todo individuo a determinarse a sí mismo, el Tribunal reconoció que adicionalmente, cada persona tenía derecho a determinarse a sí misma respecto de la divulgación y el uso de sus datos personales, esto es, a la autodeterminación informativa.⁴³

³⁸ Tribunal Constitucional Alemán, Sentencia del 15 de diciembre de 1983, BVerfGE 65,1 – Censo, diciembre 15 de 1983, versión traducida a inglés, <http://www.servat.unibe.ch/dfr/bv065001.html>

³⁹ Ibid., “2. *Limitations of this right to "informational self-determination" are only permitted in the overriding public interest. They require a constitutional legal basis, which must correspond to the rule of law of the standard clarity. In its regulations, the legislator must also observe the principle of proportionality. He also has organizational and procedural provisions to make, which counteract the danger of a violation of personal rights. For the rest, the constitutional complaints are rejected.*”

⁴⁰ Ibid., “*In its regulations, the legislator must also observe the principle of proportionality. He also has organizational and procedural provisions to make, which counteract the danger of a violation of personal rights.*”

⁴¹ Ibid.

⁴² Gerrit Hornung, Christoph Schnabel, “*Data Protection in Germany I: The Population Census Decision and the right to information and self-determination*”, *Computer Law and Security Report*, Universidad de Kessel, Alemania, 25 no. 1, (229): 4, <https://doi.org/10.1016/j.clsr.2008.11.002> : “*In this decision, the Bundesverfassungsgericht “invented” the new basic right of informational self-determination, which is the legal anchor for data protection in the German constitution*”.

⁴³ Tribunal Constitucional Alemán, Sentencia del 15 de diciembre de 1983, BVerfGE 65,1 – Censo, diciembre 15 de 1983, versión traducida a inglés, <http://www.servat.unibe.ch/dfr/bv065001.html>, “*Under the conditions of modern data processing, the protection of individuals against unlimited collection, storage, use and disclosure of their personal data is covered by the general right to privacy of Art. 2 (1) Basic Law in conjunction with Art. 1 (1) Basic Law. In this respect, the fundamental right guarantees the individual's power to determine himself, in principle, about the disclosure and use of his personal data.*”

Estos conceptos tuvieron un gran impacto en Alemania.⁴⁴ Tanto así, que Ley Federal de Protección de Datos de 1977 tuvo que ser reconsiderada, y eventualmente remplazada por la Ley Federal de Protección de Datos del 20 de diciembre de 1990, el censo de 1983 fue declarado parcialmente inconstitucional y no se llevaría a cabo un nuevo censo sino hasta 1987.⁴⁵

Es necesario considerar las razones por las que el censo de 1983 fue recibido de una manera tan negativa. Gerrit Hornung y Christoph Schnabel explican en un artículo sobre protección de datos en Alemania, que la iniciativa del Gobierno Federal de llevar a cabo este censo generó gran resentimiento en la población.⁴⁶ Lo anterior ocurrió debido a una serie de factores, dentro de los cuales se resaltan el miedo generalizado a la vigilancia estatal y la concepción de una violación injustificada a la privacidad personal.⁴⁷ Adicional a esto, la planificación del censo tuvo lugar en vísperas de 1984, año al que se le atribuyó un alto valor simbólico por la obra de George Orwell del mismo nombre.⁴⁸

Alvar y Trixy Freude de la Fundación Bertelsmann, explican que la historia alemana tuvo una incidencia directa en su política de protección de datos personales.⁴⁹ Ya se ha hecho mención del uso información estadística sobre la población alemana empleada durante el holocausto.⁵⁰ Sumado a esto, los autores mencionan que las técnicas de vigilancia estatal que eran empleadas por la policía secreta el Gobierno de Alemania Oriental fueron también un factor influyente en

⁴⁴ Ibid., 4.

⁴⁵ Ibid.

⁴⁶ Ibid., 1.

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ Alvar Freude, Trixy Freude, “*Echoes of History: Understanding German Data Protection*”, Bertelsmann Foundation, octubre de 2016, <https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/>, “*There are historical explanations for the distrust and revulsion Germans feel toward state surveillance, which help explain the widespread belief that privacy merits special protection.*”

⁵⁰ Ver Capítulo 2, Sección ii: *Antecedentes en el tratamiento automatizado de datos personales.*

la política moderna de protección de datos en este país.⁵¹ Para la Stasi⁵² era habitual implantar micrófonos en las casas de civiles, inspeccionar su correo, mantener registros sobre los habitantes que convivían en una misma dirección, sobre sus actividades, y guardar perfiles sobre personas que podrían considerarse como peligrosas o “sospechosas”.⁵³

Olivia Waxman, periodista en la Revista Time, publicó un artículo en el que explicó cómo la historia alemana tiene cierto grado de influencia en las estrictas regulaciones modernas de protección de datos, no solo de Alemania, sino en general en la legislación europea.⁵⁴

Waxman explica que, habiendo culminado el régimen de la Alemania Nazi y posteriormente el régimen de la República Democrática Alemana, como parte de la reunificación de 1990, todos los ciudadanos alemanes adquirieron los mismos derechos y libertades.⁵⁵ Sumado a esto, el fin de la Guerra Fría coincidió con un momento de auge en el intercambio de datos a lo largo de distintos países en Europa.⁵⁶ Para Waxman, lo anterior, junto con la necesidad de la Unión Europea de unificar varios países bajo un mismo mercado, es la razón por la que la primacía de la privacidad personal en materia de datos se convirtió en la regla general en Europa.⁵⁷

⁵¹ Alvar Freude, Trixy Freude, “*Echoes of History: Understanding German Data Protection*”, Bertelsmann Foundation, octubre de 2016, <https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/>

⁵² El órgano de inteligencia de la República Democrática Alemana.

⁵³ Ibid., “*The Stasi searched private premises, installed hidden tapping devices, questioned neighbors and combed the personal mail of “suspicious persons,” usually opponents of the regime. Surveillance, control and intimidation were commonplace. Logs known as “house books” showed just how deeply the state intruded into the privacy of its citizens. Beginning in the mid-1960s, every house was required to keep a record with details about each resident, including place of birth and profession. Likewise, information about any visitors had to be entered in these books. The Stasi also created files on hundreds of thousands of citizens. In particular, outside influences were considered dangerous and suspicious.*”

⁵⁴ Olivia Waxman, “*The GDPR in Just the Latest Example of Europe’s Caution on Privacy Rights. That Outlook Has a Disturbing History*”, *Time Magazine*, mayo 24 de 2018, <http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>

⁵⁵ Ibid., “*All German citizens became entitled to those rights after the reunification of Germany in 1990. The end of the Cold War coincided with the rise in data transfers throughout Europe in the ’90s. The process of establishing a single market also included a 1995 E.U. data protection regulation, and cautious attitudes about privacy became a European norm.*”

⁵⁶ Ibid.

⁵⁷ Ibid.

Siguiendo esta línea, eventualmente serían aprobadas la Directiva de Protección de Datos de 1995 y el Reglamento General de Protección de Datos de 2018.⁵⁸

Respalda lo anterior Ana Bradford, directora del Centro de Estudios Europeos de la facultad de derecho de la Universidad de Columbia, quien explica que la adopción del Reglamento General de Protección de Datos de 2018 también se debe, en parte, a la comprensión de la comunidad europea de la historia alemana.⁵⁹

Teniendo en cuenta las aproximaciones anteriormente expuestas, podría llegar a considerarse que la historia alemana efectivamente tuvo cierto grado de influencia en la implementación de legislaciones de protección de datos europeas a lo largo de la historia, incluidas la Directiva de Protección de Datos de 1995 y el Reglamento General de Protección de Datos de 2018. Debe notarse también que Alemania fue el primer país de Europa en acoger el nuevo Reglamento.⁶⁰

Lo anterior puede generar serias preocupaciones si se tiene en cuenta que países por fuera de Europa, cuyo contexto histórico y económico son muy diferentes, están empezando a adoptar legislaciones que contienen normas muy similares a las europeas.⁶¹

⁵⁸ Ibid.

⁵⁹ Ana Bradford, citada por Olivia Waxman, “*The GDPR in Just the Latest Example of Europe’s Caution on Privacy Rights. That Outlook Has a Disturbing History*”, Time Magazine, mayo 24 de 2018, <http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/> “*The understanding [of the Nazi history] is very widespread now,*” she says. “*Given the historical backdrop, that made the legislation intuitively more appealing and less subject to resistance.*”

⁶⁰ Lennart Schüßler, Natallia Karniyvich, “*Germany is the First EU Member State to enact new Data Protection Act to align with the GDPR*”, Bird & Bird, julio de 2017, <https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr>

⁶¹ Lothar Determann, “*Big Data, Economía Naranja y Machine Learning*”, 24 de enero de 2019, conferencia dictada en el 1^{er} Foro del Centro de Estudios en Derecho del Entretenimiento, Tecnología e Información, Pontificia Universidad Javeriana, Bogotá D.C., Colombia.

Más adelante se estudiará con mayor profundidad cuál es el impacto que puede llegar a tener el Reglamento desde un punto de vista distinto al de la privacidad personal, como son el desarrollo de nuevas tecnologías y nuevos mercados en el marco de la libre competencia económica.

A continuación, se expondrán algunas generalidades sobre el mercado de datos europeo para efectos de plantear la pregunta de investigación.

iv) Noción de datos personales como un mercado

En esta sección, se procederá a explicar algunos de los puntos importantes que serán tenidos en cuenta a lo largo del trabajo de investigación respecto de la noción de datos personales como un mercado. Para estos efectos, se emplearán algunos de los conceptos desarrollados en un estudio llevado a cabo por la Comisión Europea en 2017 sobre el mercado de datos europeo. Entre estos, se incluyen las *empresas de datos* y las *empresas usuarias de datos*, así como las diferentes etapas que componen una cadena de valor, reconocida también en este estudio.

En este orden de ideas, debe tenerse en cuenta que el mercado de datos es el lugar en que los agentes pueden comprar y vender datos, usualmente a través de medios electrónicos.⁶² Es aquel en el que los datos son intercambiados en la forma de productos, o en el que se prestan servicios relacionados con estos.⁶³

⁶² Margaret Rouse, “*Data Marketplace*”, Whatis.com, abril de 2015, <https://whatis.techtarget.com/definition/data-marketplace-data-market>

⁶³ Comisión Europea, Dirección General de Comunicaciones, redes, contenidos y tecnología, “*European Data Market*”, 24-25, febrero de 2017, https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1

Dentro de este, vale la pena diferenciar dos agentes diferentes; las *empresas de datos* y las empresas que son *usuarias de datos*. Las primeras son aquellas que, por lo general, representan el mercado desde el punto de vista de la oferta: su actividad económica principal consiste en la producción y prestación de servicios de datos.⁶⁴ Tal es el caso de Snowflake Inc., una compañía estadounidense, también conocida por su nombre comercial como Snowflake Computing, cuyas actividades económicas principales incluyen la prestación de servicios de almacenamiento y análisis de Big Data.⁶⁵ Las segundas, son aquellas cuya actividad económica principal no implica la producción ni prestación de servicios de datos, pero dependen significativamente de estos para cumplir con sus fines, abarcando un amplio rango de compañías en todos los sectores de la economía.⁶⁶ Son, por lo general, aquellas que representan el lado de la demanda del mercado.⁶⁷

Cabe observar que, en estos mercados, no siempre existe una diferencia tajante entre quienes son oferentes y demandantes, pues una empresa *usuaria* de datos puede eventualmente vender la información recolectada de sus clientes.⁶⁸

Adicionalmente, es necesario tener en cuenta que el hecho de ser *usuarias* no necesariamente las excluye de realizar algunas de las actividades que realizan las compañías de datos.⁶⁹ Esto se debe a que, por ejemplo, una compañía usuaria puede recolectar información acerca de sus clientes, para organizarla y analizarla por sí misma, con el fin de mejorar sus ventas o su

⁶⁴ Ibid., 25.

⁶⁵ “*About Snowflake*”, Snowflake, no hay fecha, <https://www.snowflake.com/about/>. La compañía fue fundada en 2012 y está domiciliada en San Mateo, California. Su razón social es Snowflake Inc. y su nombre comercial es Snowflake Computing. Aunque su actividad económica principal es la del almacenamiento de datos en la nube (Data Warehousing), esta también presta servicios de análisis de toda clase de datos (Big Data Analytics).

⁶⁶ Ibid., 78

⁶⁷ Ibid: “*As such, data users represent the demand side of the data market.*”

⁶⁸ Ibid., 79, “*The boundaries between demand and supply are not so clear-cut, since the companies which develop a good capability to exploit their own data may become in turn resellers of their own data to third parties*”.

⁶⁹ Ibid.

negocio en general.⁷⁰ No obstante, dicha actividad no es la actividad económica principal de la compañía usuaria.⁷¹

Como se mencionaba en la introducción a esta sección, para efectos de este trabajo de investigación, se tendrán en cuenta las etapas de la cadena de valor reconocidas por la Comisión Europea en su estudio del mercado de datos, las cuales consisten en: (i) Recolección y creación de datos, (ii) almacenamiento, agregación y organización de datos, (iii) análisis, tratamiento, mercadeo y distribución, y (iv) uso y reutilización.⁷²

La primera etapa consiste en la recolección directa, como ocurriría con la información que tienen las cadenas de *retail* sobre sus clientes, o indirectamente, como ocurre con los servicios de localización en un dispositivo móvil.⁷³ La segunda etapa es llevada a cabo tanto por proveedores especializados y redes sociales, como por compañías más tradicionales como las del sector financiero, que almacenan grandes cantidades de información sobre sus clientes.⁷⁴ La tercera etapa consiste en juntar las fuentes de información para ser analizada y así generar valor en la misma para ser distribuida.⁷⁵ Los agentes que se encargan de esta etapa pueden ser los mismos encargados de su almacenamiento en la segunda etapa, siempre que cuenten con los recursos necesarios para ello, de lo contrario, pueden contratar con un tercero para la prestación del servicio.⁷⁶ Finalmente, respecto de la etapa de uso y reutilización, la Comisión reconoce dos propósitos principales; el de hacer a la empresa u organización más eficiente, o el de brindar un mejor servicio a los clientes.⁷⁷ En este punto, se le puede dar un uso a la

⁷⁰ Ibid.

⁷¹ Ibid.

⁷² Ibid., 28. Ver “*Figure 1: The Data Value Chain and the Data Ecosystem*”.

⁷³ Ibid., 28

⁷⁴ Ibid.

⁷⁵ Ibid.

⁷⁶ Ibid., 29: “*Usage, both in the public and private sectors, to better serve customers and/or improve efficiency.*”

⁷⁷ Ibid.

información para la cual fue recolectada o, al contrario, se puede reutilizar con fines diferentes.⁷⁸

Para el primer caso, serviría el ejemplo de la información sobre el consumo de datos de un usuario de los servicios de un operador de telefonía celular para efectos de emitir una factura electrónica. Para el segundo, cuando esa misma información es utilizada con el fin de determinar los movimientos de una persona para una compañía de *retail*, para efectos como los de enviar información publicitaria a la persona.⁷⁹

Con base en los planteamientos anteriores, finaliza la sección introductoria del trabajo de investigación. A continuación, se procederá a exponer algunas generalidades sobre el Reglamento General de Protección de Datos de la Unión Europea, desde el trámite legislativo que dio lugar a su implementación y los fundamentos detrás de ésta, hasta una breve mención sobre los principales cambios que el mismo trajo consigo en materia de protección de datos. También se harán algunas aproximaciones sobre su posible efecto en materia de libre competencia económica, antes de entrar al estudio del artículo 22 del Reglamento.

3. Reglamento General de Protección de Datos de la Unión Europea

i) Antecedentes y fundamentos para la adopción de la Regulación

En esta sección se expondrán algunas de las consideraciones que fueron tenidas en cuenta para justificar la adopción del Reglamento General de Protección de Datos de la Unión Europea.

⁷⁸ Ibid.

⁷⁹ Ibid.

Adicionalmente, se hará un breve recuento del trámite legislativo llevado a cabo para su implementación, en reemplazo de la Directiva de Protección de Datos de la Unión Europea de 1995. Cabe señalar que esta Directiva no contaba con las altas sanciones que pueden ser impuestas actualmente por el Reglamento. Tampoco contaba con una aplicación extraterritorial de las normas a individuos en países por fuera de la Unión, ni con varias obligaciones en cabeza de los responsables del tratamiento que hoy en día les son exigibles. En el mismo tampoco se regularon los derechos de acceso, de supresión ni de supresión. Los derechos anteriores se encuentran consagrados en las normas del Reglamento, y serán explicados con mayor profundidad en la siguiente sección.

a. Reemplazo de la Directiva de Protección de Datos de 1995

La Directiva de Protección de Datos de 1995 (EU 95/46 de 1995) fue reemplazada en 2018 por el Reglamento General de Protección de Datos (EU 2016/679).⁸⁰ Esta iniciativa legislativa tuvo su origen varios años atrás, cuando la Comisión Europea presentó un primer borrador del nuevo Reglamento en enero de 2012.⁸¹ Esta propuesta tuvo como fundamento diferentes razones. Dentro de estas cabe resaltar el rápido avance en la tecnología, los retos que dicho avance representaba para la protección de datos personales, y la necesidad de generar confianza en los consumidores:

“La rápida evolución tecnológica ha supuesto nuevos retos para la protección de los datos personales. Se ha incrementado enormemente la magnitud del

⁸⁰ Andrew Rossow, “*The Birth of the GDPR: What Is It And What You Need To Know*”, Forbes, mayo de 2018, <https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#729a199055e5>

⁸¹ Hunton and Williams, “*The Proposed EU General Data Protection Regulation A guide for in-house lawyers*”, junio de 2015, 3, <https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2015/06/Hunton-Guide-to-the-EU-General-Data-Protection-Regulation.pdf>

intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social.

*Generar confianza en el entorno en línea es esencial para el desarrollo económico. La falta de confianza hace que los consumidores vacilen a la hora de adquirir productos en línea y adoptar nuevos servicios, con lo que se corre el riesgo de que se ralentice el desarrollo de usos innovadores de las nuevas tecnologías. (...)*⁸²

La exposición de motivos evidencia también una necesidad identificada por la Comisión de que las personas tuviesen control sobre sus datos personales:

“Si bien el marco jurídico actual sigue siendo adecuado por lo que respecta a sus objetivos y principios, no ha evitado, sin embargo, la fragmentación en cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea. Ha llegado por ello el momento de establecer un marco más sólido y coherente en materia de protección de datos en la UE, con una aplicación estricta que permita el desarrollo de la economía digital en el mercado interior, otorgue a los

⁸² Parlamento Europeo, Propuesta del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, (COM/2012/011 final-2012/0011), <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012PC0011&from=EN>

*ciudadanos el control de sus propios datos y refuerce la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas.”*⁸³

A primera vista, se observa que para la Comisión era fundamental generar confianza en el público, con el fin de desarrollar de la economía digital y una mayor innovación tecnológica.

La propuesta fue recibida por el Parlamento Europeo, el cual publicó su versión del texto con modificaciones el 12 de marzo de 2014 para ser enviado al Consejo de la Unión Europea.⁸⁴

Después de varias reuniones formales de trílogo,⁸⁵ el 8 de abril de 2016 el texto final fue aprobado por el Consejo de la Unión Europea, y el 16 de abril por el Parlamento Europeo.⁸⁶

El Reglamento General de Protección de Datos entró en vigor para los estados miembros de la Unión el 25 de mayo de 2018.⁸⁷

b. Fundamento en los Considerandos

El Considerando 171 del Reglamento General de Protección de Datos establece:

“La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su

⁸³ Ibid.

⁸⁴ “*Timeline of Events*”, EU GDPR, no hay fecha, <https://eugdpr.org/the-process/timeline-of-events/>

⁸⁵ “*Interinstitutional negotiations for the adoption of EU legislation*”, European Parliament, no hay fecha, <http://www.europarl.europa.eu/ordinary-legislative-procedure/en/interinstitutional-negotiations.html>

⁸⁶ “*Timeline of Events*”, EU GDPR, no hay fecha, <https://eugdpr.org/the-process/timeline-of-events/>

⁸⁷ “*The General Data Protection Regulation applies in all Member States from 25 May 2018*”, Eur-Lex, no hay fecha, <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html>

entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.”⁸⁸

Fue así como, a partir de su entrada en vigor, la directiva de 1995 fue derogada por completo y el Reglamento entró a regir en su lugar. A continuación, se procederá a analizar algunas de las generalidades del Reglamento.

ii) Generalidades sobre el nuevo Reglamento

En esta sección, se expondrán algunas nociones generales sobre el Reglamento General de Protección de Datos de la Unión Europea, haciendo una primera aproximación a ciertas disposiciones que pueden ser motivo de controversia, antes de entrar de fondo en el estudio del artículo 22. Para ello, en primer lugar, se hablará del incremento en las sanciones que pueden ser impuestas por incumplir con el Reglamento. También se hablará de la aplicación extraterritorial del mismo, y la posibilidad de sancionar a individuos por fuera de la Unión Europea. Con posterioridad, se mostrarán algunas de las definiciones contenidas en del Reglamento para efectos de dar mayor claridad al presente trabajo de investigación.

⁸⁸ Parlamento Europeo, Considerando 171 del Reglamento General de Protección de Datos, (EU 2016/679), abril 27 de 2016, <http://www.privacy-regulation.eu/es/r171.htm>

Finalmente, se hablará sobre algunos derechos introducidos por el Reglamento en favor de los interesados, como son el *derecho de acceso*, el *derecho de supresión*, y el *derecho de portabilidad de datos*. Frente a este último, se harán algunas observaciones desde la perspectiva de la libre competencia económica.

Lo primero que debe tenerse en cuenta es que, desde su entrada en vigencia, el Reglamento ha sido considerado como una de las regulaciones más estrictas en materia de protección de datos en el mundo.⁸⁹ Es conocido también como el más importante cambio en materia de protección de datos en Europa de los últimos veinte años.⁹⁰ A un año de su entrada en vigencia, Microsoft Corporation,⁹¹ lo describió como un marco de innovación que ha permitido el progreso en materia de privacidad.⁹²

No obstante, desde otras perspectivas se ha considerado que la implementación del Reglamento trae potenciales consecuencias adversas.⁹³

Se ha argumentado que su cumplimiento puede representar un mayor costo para las compañías medianas y pequeñas, en la medida en que sus recursos y presupuesto en ocasiones no es suficiente para cumplir algunas de las nuevas exigencias.⁹⁴ Se ha encontrado que actualmente

⁸⁹ Matt Burges, “*What is GDPR? The summary guide to GDPR compliance in the UK*”, Wired, enero de 2019, <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>

⁹⁰ “*The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years*”, EU GDPR, no hay fecha, <https://eugdpr.org/>

⁹¹ “*Microsoft Services Agreement*”, Microsoft, no hay fecha, <https://www.microsoft.com/en/servicesagreement/>, Microsoft Corporation es una compañía estadounidense domiciliada en Redmond, Washington. Su actividad económica principal es la producción de bienes y servicios en el sector de la tecnología en la mayoría de los países del mundo. Se le conoce por su nombre comercial simplemente como “Microsoft”.

⁹² Julie Brill, “*GDPR’s first anniversary: A year of progress in privacy protection*”, Microsoft, mayo de 2019, <https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/>

⁹³ Forbes Technology Council, “*15 Unexpected Consequences of the GDPR*”, Forbes, agosto de 2018, <https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#42d3f64094ad>

⁹⁴ Ibid.

millones de compañías lo incumplen.⁹⁵ Igualmente, se considera que el mismo trae consigo una inhibición en el desarrollo de nuevas tecnologías, en la medida en que varias compañías podrían tornarse más aversas al riesgo debido a las elevadas sanciones por incumplimiento.⁹⁶ Por otro lado, se ha explicado que el tratamiento de Big Data puede verse atrasado en la medida en que no es posible la toma de decisiones automatizadas que puedan tener efectos *significativos* sobre los interesados.⁹⁷ Se ha opinado también sobre la ambigüedad y la vaguedad del lenguaje empleado por este en varias de sus disposiciones.⁹⁸

Independientemente de esta discusión, vale la pena hacer mención de importantes cambios que introduce el Reglamento a la legislación europea de protección de datos.

En primer lugar, hay un incremento en los montos de las sanciones que pueden ser impuestas a compañías por infringir sus disposiciones. El artículo 83 proporciona guías bajo las cuales se deben imponer las sanciones, teniendo en cuenta elementos como la gravedad de la infracción, la intención del infractor, y el nivel de cooperación que tenga con las autoridades.⁹⁹

⁹⁵ “*Millions of small companies aren’t GDPR compliant.*”, GDPR EU, no hay fecha, <https://gdpr.eu/2019-small-business-survey/>

⁹⁶ Parlamento Europeo, Comisión Europea, Reglamento General de Protección de Datos, (EU 2016/679), mayo 25 de 2018, Art. 83, Num. 4, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>, “*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.*” (**En adelante será referido como “Reglamento”**).

⁹⁷ Samuel Greengard, “*Weighting the impact of GDPR*”, *Communications of the ACM*, 61 no. 11, (2018), 16, <https://cacm.acm.org/magazines/2018/11/232192-weighting-the-impact-of-gdpr/fulltext>, “*Other sources of uncertainty include the compatibility of GDPR with big data, and the rules concerning automated decision-making. Article 22 of GDPR states individuals have the right to “not be subject to a decision based solely on automated processing, including profiling.”*”

⁹⁸ Allison Cool, “*Europe’s Data Protection Law is a Big, Confusing Mess*”, *New York Times*, mayo de 2018, <https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html>

⁹⁹ Reglamento, Art. 83, Num. 2.

Las multas máximas que pueden ser impuestas por violaciones a las disposiciones señaladas en el artículo 83 pueden alcanzar una suma de hasta 20.000.000 de Euros, o el 4% de los ingresos totales anuales mundiales de la vigencia fiscal anterior del infractor.¹⁰⁰ Este es un cambio importante en la medida en que la Directiva 95/46 CE no imponía realmente criterios de graduación de las sanciones, ni disposiciones sobre los montos aplicables de las mismas, sino que se limitaba a remitir la facultad sancionatoria a los Estados miembros.¹⁰¹

Como se mencionaba anteriormente, el monto de las sanciones puede ser un desincentivo para las empresas más pequeñas para entrar a este mercado, pues implica mayores costos y procedimientos más complejos de cumplimiento.¹⁰² En este caso nos referimos tanto a empresas usuarias, como a empresas de datos pues, como se expuso en el capítulo introductorio, las compañías usuarias están en capacidad de realizar las mismas actividades de las compañías de datos, sin que ello signifique que se trate de su actividad económica principal.

Otro cambio importante está relacionado con la aplicación territorial del Reglamento. El mismo aplica al tratamiento de datos personales de sujetos que se encuentran en la Unión Europea, por parte de personas que no necesariamente están situadas en un país de la Unión.¹⁰³ Lo anterior amplía significativamente su aplicación territorial, y lo extiende a cualquier persona, sea natural o jurídica, sin importar si la misma se encuentra en territorio europeo, o no.¹⁰⁴ Se trata también de un concepto que no estaba incluido en la Directiva de Protección de Datos de 1995.

¹⁰⁰ Reglamento, Art. 83, Num. 5.

¹⁰¹ Parlamento Europeo, Comisión Europea, Directiva de Protección de Datos, (95/46/EC), diciembre 13 de 1995, Art. 83, Num. 4, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>

¹⁰² Raad Ahmed, “*GDPR: What Small Businesses Need To Know*”, Forbes, marzo de 2019, <https://www.forbes.com/sites/theyec/2019/03/04/gdpr-what-small-businesses-need-to-know/#54e94f373197>

¹⁰³ Reglamento Art. 3, Num. 3.

¹⁰⁴ *Ibid.*, Art. 3. Num. 2 y 3.

Para efectos de lograr una mayor claridad en el presente trabajo de investigación, en seguida se mostrarán algunas de las definiciones contenidas en el Reglamento.

Para referirse a los términos “*data processing*” y “*controller*”, los términos “*tratamiento de datos*” y “*responsable del tratamiento*” son empleados en la versión oficial en español del Reglamento.¹⁰⁵

El mismo define responsable del tratamiento como:

“(...) la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.”¹⁰⁶

En este sentido, para efectos del presente trabajo de investigación, se tendrán como responsables del tratamiento tanto a las compañías de datos como a las compañías que son usuarias de datos, pues ambos están en capacidad de ser la parte oferente del mercado de datos, y por lo tanto, determinar los fines y medios del tratamiento.

Por otro lado, define tratamiento de datos como:

“(...) cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización,

¹⁰⁵ Ibid., Art. 4. Num. 2 y 7.

¹⁰⁶ Ibid., Art. 4, Num 7.

comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.”¹⁰⁷

El Reglamento también se refiere al término “*data subject*” como el “*interesado*”, sin proveer una definición expresa para dicho término.¹⁰⁸ No obstante, de la definición de “*datos personales*” que incluye el Reglamento, se puede extraer la siguiente definición:

“datos personales”: toda información sobre una persona física identificada o identificable (**“el interesado”**) (...).¹⁰⁹ (Resaltado fuera del texto original).

De esta forma, para los efectos del reglamento, puede entenderse por interesado toda persona natural a la que se refiere la información, siendo necesario que la persona natural se encuentre identificada o que sea identificable.

Los anteriores serán los términos empleados al referirse al contenido del Reglamento, con el fin de lograr un estudio más preciso del mismo.

Por otro lado, es necesario resaltar algunos de los derechos son consagrados en favor de los interesados, así como obligaciones impuestas en los responsables del tratamiento. El artículo 33 establece que los responsables están obligados a notificar a las autoridades correspondientes en un plazo no mayor a 72 horas sobre cualquier violación en la seguridad de los datos que guarda sobre los interesados, salvo que no represente un riesgo para los derechos y libertades de las personas naturales.¹¹⁰ Igualmente, el artículo 34, establece que ante este tipo de

¹⁰⁷ Ibid., Art. 4, Num 2.

¹⁰⁸ Ibid., Art. 4, Num. 8.

¹⁰⁹ Ibid., Art. 4, Num. 1.

¹¹⁰ Ibid., Art. 33

violaciones de seguridad, se debe notificar al interesado, salvo que se hayan tomado ciertas medidas establecidas en el numeral tercero del artículo.¹¹¹

Las notificaciones al interesado no se limitan a las violaciones de seguridad. El artículo 15 del Reglamento consagra el “*derecho de acceso del interesado*”.¹¹² Este consiste en que todo interesado tiene derecho a obtener confirmación por parte del Responsable sobre si sus datos personales están siendo tratados, y en dicho caso, el derecho a tener acceso a los mismos, a saber cuáles son los fines por los que están siendo tratados, la categorización que se les está dando a sus datos personales, los destinatarios o las categorías de destinatarios a los que han sido o serán comunicados, a que los mismos sean rectificados o suprimidos, a solicitar limitaciones en su tratamiento, a presentar reclamaciones ante la autoridad, a obtener información sobre la forma en que fueron obtenidos, y si los mismos son base de toma de decisiones automatizadas en los términos del artículo 22, el cual será estudiado con mayor profundidad más adelante.¹¹³

El Reglamento hace especial énfasis en el derecho de supresión que tiene el interesado, en inglés “*erasure*”, también conocido como derecho al olvido.¹¹⁴ Este se materializa en la facultad del interesado de solicitar que se eliminen sus datos personales de los servidores del responsable del tratamiento, y en la obligación de este a hacerlo en sin dilaciones indebidas,

¹¹¹ Ibid., Art. 34, “*a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.*”

¹¹² Ibid., Art. 15.

¹¹³ Ibid., Art. 15, Num. 1.

¹¹⁴ Ibid., Art. 17.

siempre que se presenten las circunstancias consagradas en el numeral 1, o que no se presenten las excepciones del numeral 3 del artículo.¹¹⁵

El Reglamento también consagra el derecho a la *portabilidad* de datos personales.¹¹⁶ En virtud de este derecho, los interesados pueden solicitar recibir la información personal entregada a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, así como a transferirlos a otro responsable.¹¹⁷ El ejercicio del derecho de la portabilidad de datos procede cuando la información ha llegado al responsable en tres escenarios: en virtud del consentimiento prestado por el interesado para el tratamiento sus datos personales,¹¹⁸ cuando fue necesario para la ejecución de un contrato¹¹⁹, y cuando el tratamiento se efectúe por medios automatizados.¹²⁰ Adicionalmente, el Reglamento establece que, si bien el interesado puede solicitar transferir la información a otro responsable, dicha solicitud solo procederá cuando ello sea “*técnicamente posible*”.¹²¹

Debido a que existen problemas de incompatibilidad entre los sistemas que manejan los distintos responsables, se ha considerado que dicha expresión podría representar grandes problemas al momento de exigir la transferencia de datos personales de un responsable al otro, pues al ser incompatibles, el responsable podría no estar obligado a transferirlos.¹²²

¹¹⁵ Ibid.

¹¹⁶ Ibid., Art. 20.

¹¹⁷ Ibid.

¹¹⁸ Entendido en los términos de los Artículos 6, Num. 1 Lit. a, y 9, Num.1, Lit a del Reglamento.

¹¹⁹ Entendido en los términos del Artículo 6, Num 1, Lit. b del Reglamento.

¹²⁰ Ibid., Art. 20.

¹²¹ Ibid., Art. 20, Num. 2.

¹²² “*The Potential Effects of Data Portability Under GDPR*”, Bradley, noviembre de 2017, <https://www.bradley.com/insights/publications/2017/11/the-potential-effect-of-data-portability-under-gdpr>, “*On the other hand, system incompatibility within and among controllers presents potential technical difficulties. The EU recognized the variance in software and technology among controllers, and not wanting to unnecessarily disrupt the global market, carved out a significant exception to the right to data portability. As set forth in subprovision 2 of Article 20, a data controller would only be required to transfer the data to another controller where the transfer is “technically feasible.” The GDPR does not define this ambiguous term and fails to specify the electronic format necessary for data portability. When coupled with the fact that the GDPR does not require*

Sumado a esto, se ha explicado que algunas pequeñas y medianas compañías no están en condiciones de cumplir con los requisitos necesarios para la transferencia de los datos a otro responsable del tratamiento.¹²³

Respecto de lo anterior, el Grupo de Trabajo de Protección de Datos del Artículo 29 de la Directiva de 1995,¹²⁴ argumentó que en la medida en que se busca la transferencia de datos personales de un responsable a otro, se está promoviendo el libre flujo de la información y fomentando la libre competencia en el mercado.¹²⁵ Sin embargo, puede que el efecto en materia de libre competencia no necesariamente sea este.

Lo anterior se debe a que, por un lado, se propicia un espacio en que algunos de los grandes competidores no estarán obligados a transferir los datos personales obtenidos debido a que el mismo artículo únicamente permite que estos sean trasladados cuando dicha transferencia sea *técnicamente posible*.¹²⁶ Grandes compañías podrían buscar excluir pequeños competidores al

a controller to adopt or maintain systems that are technically compatible with a competitor's, the shortcomings of the right to data portability become apparent."

¹²³ Aysem Diker Vanberg, Mehmet Bilal Ünver, "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?", *European Journal of Law and Technology*, 8 no. 1 (2017): 4, <http://ejlt.org/article/view/546/727>, "Article 20 of the GDPR requires an online service to write specialised code (export-import module, (EIM)) that will export data from that service and import it to another service. As noted by Swire and Lagos, many small and medium-sized companies do not have the resources to fully understand the GDPR, comply with it and write an EIM to move data to another provider."

¹²⁴ Comisión Europea, Grupo de Trabajo del Artículo 29, "Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679", Revisadas por última vez por el Grupo el 6 de febrero de 2018, 1, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053,

"Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos e intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE."

¹²⁵ Comisión Europea, Grupo de Trabajo del Artículo 29, "Directrices sobre el derecho a la portabilidad de datos del Reglamento 2016/679", Revisadas por última vez por el Grupo el 6 de febrero de 2018, 24, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233, "Puesto que permite la transmisión directa de datos personales de un responsable del tratamiento a otro, el derecho a la portabilidad de los datos es también una herramienta importante que respaldará la libre circulación de datos personales en la UE y promoverá la competencia entre los responsables del tratamiento. Facilitará el cambio entre distintos proveedores de servicios y, por lo tanto, promoverá el desarrollo de nuevos servicios en el contexto de la estrategia para el mercado único digital."

¹²⁶ Reglamento, Art. 20, Num. 2.

rehusarse a compartir los datos, de lo cual podría derivarse un abuso de su posición dominante, en los términos del artículo 102 del TFUE.¹²⁷

Por otro lado, se podrían estar imponiendo barreras de entrada al mercado de datos a las compañías que no son capaces de transferir los datos siguiendo las especificaciones del Reglamento.¹²⁸ Que se les exija un módulo exportación/importación (EIM), así como el código necesario para poder implementarlo, implica un aumento significativo en los costos para compañías pequeñas y medianas,¹²⁹ el cual puede dificultarles entrar o permanecer en el mercado, y por lo tanto, reducir la competencia y el nivel de innovación en el mismo.¹³⁰

Expuestas algunas de las generalidades del Reglamento en materia de derechos y obligaciones, es posible afirmar que se trata de un reglamento enfático en la protección de los derechos de los interesados. No obstante, es claro que es también un reglamento exigente para los responsables del tratamiento.

¹²⁷ Aysem Diker Vanberg, Mehmet Bilal Ünver, “*The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*”, *European Journal of Law and Technology*, 8 no. 1 (2017): 8, <http://ejlt.org/article/view/546/727>, “(...) it can be argued that a refusal of a dominant firm to enable data portability might be seen as a form of exclusionary abuse as it might drive its competitors out of a specific relevant market and increase market concentration.”

¹²⁸ Ibid., 4, “Article 20 of the GDPR requires an online service to write specialised code (export-import module, (EIM)) that will export data from that service and import it to another service. As noted by Swire and Lagos, many small and medium-sized companies do not have the resources to fully understand the GDPR, comply with it and write an EIM to move data to another provider.”

¹²⁹ Ibid.

¹³⁰ Ibid., “Whilst such costs may not be significant for large companies, the requirement is likely to create problems for small and medium-sized companies. It must be noted that complying with the GDPR should not to be taken lightly due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 per cent of the total worldwide annual turnover of the preceding year, whichever is greater.

The issue of disproportionate costs was also raised in December 2015 by Baroness Neville Rolfe, the UK's parliamentary Under-Secretary of State for the Department for Business, Innovation and Skills. She stated that data portability rules designed to enable consumers to move their data from one platform to another should not be too costly as they can serve as an entry barrier into markets, and this might have an adverse effect on innovation and competition.”

Lo anterior permite evidenciar que la adopción de algunos artículos podría estar generando factores adversos que no están siendo tenidos en cuenta.

Su implementación puede dar inicio a un debate sobre si el Reglamento podría estar creando escenarios que faciliten a algunos de los responsables del tratamiento abusar de su posición dominante,¹³¹ y que compañías más pequeñas, usuarias y de datos, se vean privadas de ingresar o permanecer en este.¹³² De ser así, contrario al argumentos que plantea el Grupo de Trabajo del Artículo 29, la forma en que el Reglamento consagra algunos derechos en favor de los interesados, podría inducir a que las compañías que hacen parte de los mercados de datos se vean forzadas a operar en un entorno en que se limiten las condiciones de libre competencia.¹³³

Uno de estos podría ser el derecho consagrado en el artículo 22 del Reglamento, que consiste en que los interesados no sean objeto de una decisión tomada a partir de medios completamente automatizados con base en sus datos personales, o la elaboración de perfiles, siempre que esta produzca efectos significativos sobre los mismos.¹³⁴

A continuación, se analizarán algunos aspectos de este artículo para determinar si, efectivamente, el mismo podría ser fuente de atraso en el desarrollo de nuevas tecnologías y generar limitantes sobre a las condiciones de libre competencia.

iii) Artículo 22

El artículo 22 del Reglamento General de Protección de Datos establece:

¹³¹ Ibid.

¹³² Ibid.

¹³³ Ibid.

¹³⁴ Reglamento, Art. 22, Num. 1.

Artículo 22

Decisiones individuales automatizadas, incluida la elaboración de perfiles

“1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o;

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. *Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.*¹³⁵

Para efectos del presente trabajo de investigación, se analizarán el concepto de toma de decisiones automatizadas, el de *profiling* o “*elaboración de perfiles*”, la noción de “*decisiones que produzcan efectos jurídicos*” o que “*lo afecten significativamente de modo similar*”, las circunstancias en las que dicho tratamiento es permitido, y las dificultades interpretativas del artículo bajo estudio.

a. Decisiones automatizadas individuales

El artículo 15 de la Directiva de Protección de Datos de 1995 también establecía el derecho a no ser sujeto de decisiones basadas exclusivamente en procesos automatizados de toma de decisiones.¹³⁶ No se trata entonces de un derecho consagrado por primera vez en la Unión Europea.

¹³⁵ Reglamento, Art. 22.

¹³⁶ Parlamento Europeo, Comisión Europea, Directiva de Protección de Datos, (95/46/EC), diciembre 13 de 1995, Art. 15, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>, “1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o

El proceso consiste en tomar una decisión a partir de medios automatizados sin intervención humana alguna, a partir de datos fácticos, perfiles sobre personas creados digitalmente o información que es inferida a partir de información recolectada anteriormente.¹³⁷

Dentro de este, pueden incluirse los lectores de exámenes académicos de respuesta múltiple que otorgan un puntaje individual, a partir del cual el mismo sistema podría aprobar o reprobar al estudiante.¹³⁸

Una importante diferencia entre la Directiva de 1995 y el Reglamento es que el segundo consagra explícitamente el derecho a no ser objeto de decisiones automatizadas, incluyendo el *profiling*.¹³⁹ En el caso de los lectores de exámenes con respuesta múltiple, se habla de una forma de toma de decisiones automatizadas pura y simple, pues la decisión no se toma a partir de la elaboración de un perfil individual, sino de la calificación necesaria para aprobar y la calificación que obtuvo el estudiante.¹⁴⁰ En la siguiente sección, el concepto de *profiling* será estudiado a mayor profundidad.

b. Profiling

Es de observar que, si bien la Directiva de 1995 no hacía mención explícita de esta forma de tratamiento, la misma sí prohibía la toma de decisiones a partir del tratamiento de datos para

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

¹³⁷ “*What is automated decision making including profiling ?*”, Information Commissioner’s Office, no hay fecha, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id2>

¹³⁸ Ibid.

¹³⁹ Reglamento, Art. 22.

¹⁴⁰ Ibid.

evaluar ámbitos muy específicos, como el desempeño de una persona en cuanto a su trabajo, su capacidad de adquirir un crédito, su fiabilidad y su conducta.¹⁴¹ De lo anterior podría interpretarse una restricción mucho más reducida y específica a la *elaboración de perfiles*, y podría ser la explicación por la cual el derecho consagrado por el artículo 15 de la Directiva rara vez fue invocado.¹⁴²

No obstante, este concepto fue introducido de manera explícita como parte del Reglamento de 2018. Consiste en una forma específica de tratamiento automatizado de datos empleado para “*derivar, inferir, predecir y evaluar información demográfica, atributos comportamentales e inclusive la identidad de las personas*”.¹⁴³ En la versión oficial en español del Reglamento se emplea el término “*elaboración de perfiles*”, y se define como:

“(…) *toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*”.¹⁴⁴

¹⁴¹ Parlamento Europeo, Comisión Europea, Directiva de Protección de Datos, (95/46/EC), diciembre 13 de 1995, Art. 15, Num. 1, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>, “*Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.*”

¹⁴² “*Data is Power: Profiling and Automated Decision-Making in GDPR*”, Privacy International, 2017, <https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr>, “In contrast to automated decision-making, a **hardly used right not to be subject to decision based solely on automated processing** in the 1996 Data Protection Directive, profiling is a relatively novel concept in European data protection regulation.”

¹⁴³ Ibid.

¹⁴⁴ Art. 4, Num. 4.

Se puede observar que un ámbito de aplicación mucho más amplio y mucho más específico de elaboración de perfiles que aquel proporcionado por la Directiva.

Las Guías sobre las decisiones individuales automatizadas y la elaboración de perfiles del Grupo de Trabajo del Artículo 29 establecen que la elaboración de perfiles en el marco del Reglamento requiere de tres condiciones: (i) debe ser una forma automatizada de tratamiento de datos, (ii) debe ser llevada a cabo respecto de información de personas naturales, y (iii) el objeto de la elaboración del perfil debe ser el de “evaluar aspectos personales” de una persona natural.¹⁴⁵

A diferencia del concepto anterior, las decisiones automatizadas a partir de la elaboración de perfiles tienen un campo de aplicación mucho más relevante en el desarrollo de nuevas tecnologías, como se explicará a continuación.

Un ejemplo de esto es el uso Machine-learning para predecir la posibilidad de que un tratamiento médico sea efectivo en un paciente con base en información recolectada sobre el mismo, y así tomar la decisión sobre si éste debiese ser tratado.¹⁴⁶ Otras aplicaciones prácticas en el campo de la medicina serán mencionadas más adelante.

El Grupo de Trabajo 29 propone algunos ejemplos como el de la venta de datos personales recolectados por un agente, que posteriormente los vende a compañías, las cuales los adquieren

¹⁴⁵ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 8, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

¹⁴⁶ “*What is automated decision making including profiling ?*”, Information Commissioner’s Office, no hay fecha, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id2>

con la finalidad de mejorar sus ventas o de enfocar su publicidad de manera más directa.¹⁴⁷ Otro es el de la información recogida por cámaras de tránsito, que al ser la única base para imponer una multa a un infractor, pueden servir como una forma de *profiling*.¹⁴⁸ Lo anterior ocurriría en la medida en que la imposición de la sanción tuviese como base factores como que el infractor sea reincidente, o que ya haya cometido distintas violaciones.¹⁴⁹

En el Considerando 171 del Reglamento, se explica que decisiones automatizadas como las de negar una solicitud en línea para adquirir un crédito, o la contratación en línea (*e-recruiting*), sin ninguna forma de intervención humana, son formas *de profiling* que recaen en el supuesto del artículo.¹⁵⁰

Otro ejemplo se presenta en el desarrollo de la industria automotriz.¹⁵¹ Más adelante se explicará como la elaboración de perfiles es necesaria para los vehículos autónomos en cuanto al desarrollo de su tecnología y en cuanto a su competitividad en el mercado.¹⁵²

¹⁴⁷ Comisión Europea, Grupo de Trabajo del Artículo 29, ““*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*””, Revisadas por última vez por el Grupo el 6 de febrero de 2018, , https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, Ver ejemplo 1.

¹⁴⁸ Ibid., ver ejemplo 2.

¹⁴⁹ Ibid.

¹⁵⁰ Considerando 171 del Reglamento General de Protección de Datos de la Unión Europea.

¹⁵¹ Chelsey Colbert, “*Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles*”, Universidad de Stanford, marzo de 2018, <https://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/47/2018/02/Privacy-Under-the-Hood-Towards-an-International-Data-Privacy-Framework-for-Autonomous-Vehicles.pdf>

¹⁵² Ver Capítulo 4, Sección i: *Usos prácticos en la actualidad y posibles usos en el futuro*.

c. Noción de “decisiones que produzcan efectos jurídicos” o “que afecten significativamente o de modo similar” al interesado

El artículo 22 da el derecho a los interesados a no ser objeto de una decisión tomada únicamente por medios automatizado con base en el tratamiento de sus datos personales, incluyendo la elaboración de perfiles, siempre que esta pueda tener efectos jurídicos sobre el interesado, o puedan afectarlo significativamente de modo similar.¹⁵³ Debe observarse que ni el Reglamento ni los Considerandos proveen una noción sobre lo que debe entenderse por “efectos jurídicos” o “afectarlo significativamente de modo similar.”

No obstante, en la Guía del Grupo de Trabajo 29 se explica de manera más detallada el significado de estos términos.¹⁵⁴ En la opinión del Grupo, para que la decisión tenga efectos jurídicos, es necesario que aquella tenga graves implicaciones para la persona, e implica también que se afecten derechos “jurídicos” de la misma, como los de la libre asociación, el de votar en unas elecciones, o el de iniciar una acción ante las autoridades judiciales.¹⁵⁵ Para el Grupo, se refiere también a una decisión que afecte el estatus legal de una persona en virtud de un contrato.¹⁵⁶

Para efectos de explicar este concepto, el Grupo proporciona tres ejemplos: (i) decisiones que den lugar a la cancelación de un contrato, (ii) que den lugar tanto a conceder como a denegar

¹⁵³ Art. 22, Numeral 1.

¹⁵⁴ Comisión Europea, Grupo de Trabajo del Artículo 29, “Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 23, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

¹⁵⁵ Ibid.

¹⁵⁶ Ibid.

beneficios sociales otorgados por ley, como las prestaciones por hijos o la ayuda a la vivienda, y (iii) que nieguen la admisión a un país o nieguen a una persona la ciudadanía.¹⁵⁷

El Grupo concibe la noción de la expresión “*que afecten significativamente o de modo similar*” como aquella que, sin producir efectos legales, aún puedan ser parte del ámbito de aplicación del artículo 22 debido al impacto que genera en el interesado.¹⁵⁸ Para el Grupo, la expresión “*de modo similar*” implica a que el alcance de la afectación debe ser similar a la de los efectos jurídicos.¹⁵⁹ Para estos efectos, establece que la decisión debe tener el potencial de (i) afectar de manera significativa las circunstancias, o las elecciones o de los individuos, (ii) tenga un impacto permanente o prolongado en el interesado, o (iii) provoque la exclusión o discriminación de personas.¹⁶⁰

Respecto de la expresión “*significativamente*”, el Grupo reconoce la dificultad de lograr mayor precisión, por lo que proporciona los siguientes ejemplos; (i) circunstancias que puedan afectar las condiciones financieras de una persona, como su aptitud para recibir un crédito, (ii) que afecten su acceso a los servicios de salud, (iii) que nieguen el acceso a oportunidades laborales o sitúe al individuo en posiciones de desventaja, y (iv) decisiones que nieguen el acceso a la educación, como las admisiones a una universidad.¹⁶¹

Más adelante, se explicará cómo lo anterior aún puede ser fuente de ambigüedad y dificultades en la interpretación de la norma.

¹⁵⁷ Ibid.

¹⁵⁸ Ibid.

¹⁵⁹ Ibid.

¹⁶⁰ Ibid.

¹⁶¹ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 24 , https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

d. Excepciones a la restricción

El numeral 2 del artículo 22 del Reglamento establece tres escenarios bajo los cuales las disposiciones del numeral primero del artículo 22 no aplican.¹⁶² Se está ante estos escenarios cuando la decisión: (i) “*es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento*”, (ii) “*está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado*”, o (iii) “*se basa en el consentimiento explícito del interesado.*”¹⁶³

Las Guías del Grupo de Trabajo aclaran respecto del literal a, que la excepción de celebración o ejecución de un contrato únicamente procede en la medida en que se demuestre que el tratamiento automatizado era “*necesario*” debido a que no existen otros medios menos invasivos para la intimidad y que en ocasiones puede resultar poco práctica o imposible una participación humana rutinaria.¹⁶⁴

Respecto del consentimiento, el mismo grupo aclaró que para que pueda ser alegado como excepción, es necesario que el mismo sea un consentimiento *explícito*, en el que al interesado entienda perfectamente a qué está accediendo.¹⁶⁵

¹⁶² Reglamento, Art. 22, Num. 2, Lit. a, b y c.

¹⁶³ Ibid.

¹⁶⁴ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 26 , https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

¹⁶⁵ Ibid., 14.

e. Dificultades interpretativas del artículo 22

Uno de los problemas que trajo consigo el nuevo Reglamento está relacionado con la dificultad interpretativa de varias de sus disposiciones, lo cual hace más difícil lograr un cumplimiento efectivo del mismo.¹⁶⁶

Antes de su entrada en vigencia, existía incertidumbre respecto de si el artículo debía leerse como un derecho de los interesados o, al contrario, como una prohibición para los responsables del tratamiento.¹⁶⁷

Lo anterior resulta relevante debido a que, de tratarse de una prohibición para los responsables, únicamente se podrían hacer efectivas las tomas de decisiones automatizadas en los términos del numeral 1 del artículo cuando los responsables actuasen amparados bajo las excepciones del numeral 2.¹⁶⁸ Sin embargo, si se interpretara como un derecho, sería necesario que los interesados objetasen la decisión cada vez que consideraran que eran sujetos de tal decisión.¹⁶⁹

El Grupo de Trabajo se encargó de poner fin a este debate al establecer en sus Guías que el artículo debe ser interpretado como una *prohibición* en la medida en que lo dispuesto por el

¹⁶⁶ “Top 5 Concerns with GDPR Compliance”, Thomson Reuters, no hay fecha, <https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance>

¹⁶⁷ Sandra Wachter, Brent Mittelstadt, Luciano Floridi, “Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, *International Data Privacy Law*, 7 no. 2, (2017), 95, <https://academic.oup.com/idpl/article-pdf/7/2/76/17932196/ix005.pdf>, “Due to the similarities of language and content between Article 15 of the Directive and Article 22 GDPR, the varying implementation of Article 15 as a prohibition or right to object by Member states supports the interpretation that Article 22 is ambiguous and can be read as a prohibition or right to object. **Resolving the ambiguity prior to 2018 is critical, as the two interpretations have very different consequences for data subjects and data controllers.**”

¹⁶⁸ Ibid.

¹⁶⁹ Ibid., “If Article 22 is interpreted as a prohibition, data controllers will not be allowed to make automated decisions about a data subject until one of the three requirements specified in Article 22(2) (necessary to enter or to perform a contract, authorized by law, or explicit consent) is met. Data subjects do not need to act to prevent automated decision-making, but are rather protected by default.... If Article 22 is interpreted as a right to object, automated decision-making is restricted only to cases in which the data subject actively objects.”

numeral 1 del artículo aplicaba independientemente de que el derecho fuese invocado por el interesado.¹⁷⁰ Aunque las Guías proporcionan una noción un poco más clara del concepto de “*efectos legales*” que trae consigo el numeral 1 del artículo, puede observarse que aún quedan algunos vacíos. De la lectura del artículo 22 y de la Guía del Grupo de trabajo, se proponen algunos de estos.

En primer lugar, la Guía explica que, para producir efectos jurídicos sobre el interesado, se entiende que es aquella decisión que afecte el estatus legal de una persona en virtud de un contrato.¹⁷¹ Sin embargo, queda la duda sobre si también incluye las decisiones que afecten el estatus legal de una persona que no surja en virtud de un contrato, sino de la ley, como ocurriría con figuras como la filiación o las relaciones de parentesco.

A primera vista, también quedaría el vacío de si por “*derechos jurídicos de una persona*” deben entenderse *todos* los derechos que puedan ser atribuidos a un ciudadano europeo. No es claro si se protegen toda clase de derechos, aquellos consagrados en virtud de tratados internacionales, si únicamente ampara derechos del orden constitucional de cada país, si están amparados derechos consagrados en la ley, o si también caben aquellos de desarrollo jurisprudencial.¹⁷²

¹⁷⁰ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 21 , https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053: “El término «derecho» de la disposición no significa que el artículo 22, apartado 1, se aplique solo cuando se invoque de forma activa por parte del interesado. El artículo 22, apartado 1, establece una prohibición general de las decisiones basadas únicamente en el tratamiento automatizado. Esta prohibición se aplica tanto si el interesado adopta una acción relativa al tratamiento de sus datos personales como si no lo hace”.

¹⁷¹ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 23 , https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, “(...) un efecto jurídico puede ser algo que afecte al estatuto jurídico de una persona o a sus derechos en virtud de un contrato.”

¹⁷² *Ibid.*, “Un efecto jurídico exige que la decisión, basada únicamente en el tratamiento automatizado, afecte a los derechos jurídicos de una persona.”

Cierto es que, si el Reglamento se refiere a *todos* los derechos, resultaría difícil concebir escenarios en los que la toma de decisiones automatizadas *no* tenga efectos jurídicos sobre el interesado. Por ejemplo, cualquier decisión que involucre el uso de los datos personales de un ciudadano alemán, y que puedan ser atribuidos al mismo, inclusive si no tiene efectos directos sobre éste, siempre afectarían su derecho a la autodeterminación informativa, el cual está consagrado jurisprudencialmente.¹⁷³ Para estos efectos, se prohibiría cualquier decisión automatizada que no cuente con su consentimiento, lo cual, como se explicará, resulta imposible en campos como los de la investigación médica, en los que no siempre se puede trabajar con información anonimizada y la información de pacientes suele ser reutilizada.¹⁷⁴

Por otro lado, puede observarse un problema en cuanto a la interpretación que hace el Grupo de Trabajo frente a este mismo numeral, en el sentido que, incluso cuando se encuentra que la afectación debe ser “*similar*” a la de los efectos jurídicos, es muy difícil medir el nivel de afectación “*grave*” al que se refiere el Grupo respecto de dichos efectos, pues la gravedad de los efectos de la decisión puede terminar siendo un concepto excesivamente subjetivo para cada individuo.¹⁷⁵ Aunque el Grupo de Trabajo indica que depende de cuando el interesado *se vea* suficientemente afectado puede exigir la protección,¹⁷⁶ ¿Cómo pueden los responsables del

¹⁷³ Tribunal Constitucional Alemán, Sentencia del 15 de diciembre de 1983, BVerfGE 65,1 – Censo, diciembre 15 de 1983, versión traducida al inglés, <http://www.servat.unibe.ch/dfr/bv065001.html>

¹⁷⁴ Ver Capítulo 4, Sección iii, Subsección a: *Posibles desincentivos para la innovación en nuevas tecnologías*. Ver también: Menno Mostert, Annelien Bredenoord, Monique Biesart, Johannes Van Delden, “*Big Data in medical research and EU data protection law: challenges to the consent or anonymize approach*”, *European Journal of Human Genetics*, 24 no. 7, (2016), 956-960, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5070890/>

¹⁷⁵ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 24, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, “(...) incluso cuando no se produzca ningún cambio en sus obligaciones o derechos jurídicos, el interesado puede verse suficientemente afectado como para exigir protección en virtud de esta disposición.”

¹⁷⁶ *Ibid.*

tratamiento determinar que el efecto producido puede ser considerado como *grave* para cada interesado, más aún cuando para ellos opera como una prohibición?¹⁷⁷

Podría generar aún mayores dificultades interpretativas la excepción consagrada en el numeral 2 del artículo, que permite que las decisiones con base en tratamiento automatizado, sean llevadas a cabo cuando ello sea necesario para la celebración o ejecución de un contrato.¹⁷⁸

¿Aplica la excepción inclusive si el derecho afectado es un derecho fundamental? Para ello, se plantea el siguiente ejemplo:

Podría entenderse que no ingresar a una universidad con base en una decisión automatizada tomada a partir del tratamiento de la información del sujeto, podría generar un efecto adverso “*significativo*” para el interesado, pues se le priva de un derecho legalmente reconocido como fundamental, que es el derecho a la educación.¹⁷⁹

Sin embargo, en caso de probar los elementos de *necesidad* que son señalados dentro de la Guía del Grupo de Trabajo del Artículo 29 para invocar la excepción,¹⁸⁰ ¿Podría la universidad alegar que está dentro del ámbito de la excepción del artículo 22 por considerarlo necesario para la celebración del contrato con el interesado? ¿Podría así vulnerar su derecho fundamental

¹⁷⁷ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 21 , https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053: “El término «derecho» de la disposición no significa que el artículo 22, apartado 1, se aplique solo cuando se invoque de forma activa por parte del interesado. El artículo 22, apartado 1, establece una prohibición general de las decisiones basadas únicamente en el tratamiento automatizado. Esta prohibición se aplica tanto si el interesado adopta una acción relativa al tratamiento de sus datos personales como si no lo hace”.

¹⁷⁸ Reglamento, Art. 22, Num 2, Lit a.

¹⁷⁹ Primera Convención Europea, Carta de los Derechos Fundamentales de la Unión Europea, 18 de diciembre de 2000, Artículo 14, http://www.europarl.europa.eu/charter/pdf/text_es.pdf

¹⁸⁰ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 14, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

a la educación? El Grupo plantea una situación similar, sin embargo, en ningún momento considera la posibilidad de estos conceptos entren en conflicto.¹⁸¹

Independientemente de la respuesta que se le pueda dar a estas contradicciones, lo cierto es que genera dificultades para los responsables del tratamiento, los cuales no siempre tienen las herramientas para interpretar la normativa que de por sí ya cuenta con un lenguaje ambiguo.¹⁸²

Tales contradicciones podrían representar un alto grado de incertidumbre en el cumplimiento del Reglamento. Puede que los órganos decisorios de una compañía tengan toda la intención de cumplir la norma. No obstante, si no hay certeza sobre cuáles son los escenarios en los que se permite la toma de decisiones y en los que no, es muy posible que algunas compañías se muestren reacias a participar en actividades que involucren el uso de los sistemas a los que se refiere el artículo 22. Esto con el fin de no arriesgarse a incurrir en una infracción y ser sancionadas. La implementación de políticas de cumplimiento, así como la designación de personas encargadas de hacer cumplir dichas políticas a nivel interno de las empresas,¹⁸³ puede representar mayores costos que no todas las empresas están preparadas para asumir.¹⁸⁴

¹⁸¹ Ibid., 25, “*Hipotéticamente, una empresa de tarjetas de crédito podría reducir el límite de la tarjeta de un cliente basándose no en el propio historial de reembolsos del cliente, sino en criterios de crédito no tradicionales, como un análisis de otros clientes que vivan en la misma zona y que compren en las mismas tiendas. Esto podría implicar que alguien se viera privado de oportunidades sobre la base de las acciones de otras personas. En un contexto diferente, el uso de estos tipos de características podría presentar la ventaja de ampliar el crédito a personas sin un historial crediticio convencional y a las que dicho aumento se les denegaría en otras circunstancias.*”

¹⁸² Sandra Wachter, Brent Mittelstadt, Luciano Floridi, “*Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*”, *International Data Privacy Law* 7 no. 2, (2017), 95, <https://academic.oup.com/idpl/article-pdf/7/2/76/17932196/ix005.pdf>, “*Due to the similarities of language and content between Article 15 of the Directive and Article 22 GDPR, the varying implementation of Article 15 as a prohibition or right to object by Member states supports the interpretation that Article 22 is ambiguous and can be read as a prohibition or right to object.*”

¹⁸³ Por ejemplo, nombrar un oficial de cumplimiento de las normas de GDPR como parte de un programa de *compliance* en normas de protección de datos.

¹⁸⁴ Aysem Diker Vanberg, Mehmet Bilal Ünver, “*The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*”, *European Journal of Law and Technology*, 8 no. 1 (2017): 4, <http://ejlt.org/article/view/546/727>, “*It must be noted that complying with the GDPR should not to be taken lightly due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 per cent of the total worldwide annual turnover of the preceding year,*

Expuestas algunas posibles ambigüedades y dificultades interpretativas, en seguida se analizará el concepto de la toma de decisiones automatizadas desde un punto de vista práctico, así como las posibles repercusiones que podría llegar a tener su limitación desde una perspectiva del desarrollo de nuevas tecnologías, el mercado de datos y la libre competencia.

4. Procesos automatizados de toma de decisiones y *profiling*

En el siguiente capítulo se presentarán algunos usos prácticos de tecnologías en diferentes industrias, cuyo desarrollo depende en gran medida de los procesos automatizados de toma de decisiones, incluyendo el *profiling*, así como los usos que podría dárseles en el futuro. Posteriormente, se mencionarán algunas de las ventajas que representan estos sistemas en términos de eficiencia y reducción de costos. Finalmente, se procederá a analizar cuales son los efectos que la restricción al uso de sistemas de toma de decisiones automatizadas podría generar en la libre competencia económica, haciendo énfasis en tres puntos: la restricción como un posible desincentivo para la innovación en nuevas tecnologías, la imposición de barreras de entrada al mercado y la mayor concentración en el mercado de datos.

i) Usos prácticos en la actualidad y posibles usos en el futuro

En esta sección se presentan algunas tecnologías cuyo desarrollo depende en gran medida de los procesos de toma de decisiones automatizadas. Para ello, se hará énfasis en el sector de los vehículos autónomos, en el sector médico y en el sector de la psicología. Finalmente, se

whichever is greater (...) As noted by Swire and Lagos, many small and medium-sized companies do not have the resources to fully understand the GDPR (...)."

mencionarán otros usos prácticos identificados por la Comisión Europea, mostrando como ésta ha reconocido el beneficio que muchos de estos trasladan a los consumidores.

Anteriormente, se hizo mención de la industria de los vehículos autónomos y la importancia que tiene la recolección y tratamiento de datos personales en materia de innovación y competitividad. Son vehículos autónomos todos aquellos que pueden trasladarse desde un punto a otro por sí solos, a partir únicamente de tecnología integrada dentro de los mismos.¹⁸⁵

De acuerdo a un estudio llevado a cabo por Intel Corporation¹⁸⁶ en 2017, se estima que la industria de los vehículos autónomos podría generarle cerca de 7 trillones de dólares a la economía global para el año 2050, así como prevenir la muerte de cerca de 585.000 personas entre los años 2035 y 2045, señalando también que el 94% de los accidentes automovilísticos se deben al error humano.¹⁸⁷

En un informe publicado en mayo de 2018, el Grupo de Consulta del Consumidor de la Comisión Europea explicó que los sistemas de toma de decisiones automatizadas ya están presentes en muchas características de seguridad y de asistencia al manejar.¹⁸⁸

¹⁸⁵ “*Autonomous Vehicles*”, Gartner, no hay fecha, <https://www.gartner.com/it-glossary/autonomous-vehicles/>

¹⁸⁶ “*Intel Terms of Use*”, Intel, no hay fecha, <https://www.intel.com/content/www/us/en/legal/terms-of-use.html>. Conocida por su nombre comercial simplemente como “*Intel*”, es una compañía estadounidense domiciliada en Santa Clara, California. Su Actividad económica principal es el desarrollo y manufactura de productos y servicios en el sector de la tecnología.

¹⁸⁷ Roger Lanctot, “*Accelerating the Future: The Economic Impact of the Emerging Passenger Economy*”, Strategy Analytics, Intel, junio de 2017, 23, https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf?cid=em-elq-26916&utm_source=elq&utm_medium=email&utm_campaign=26916&elq_cid=1494219

¹⁸⁸ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “*Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world*”, mayo de 2018, 8, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf, “*Today’s cars already dispose of sensors that, in combination with cruise control and road marking recognition keep the vehicle automatically at a specific distance from other vehicles. Similar sensors allow to recognise pedestrians and brake autonomously.*”

La recolección de datos personales sobre los usuarios que manejan automóviles inteligentes puede ser útil para desarrollar tecnologías que permitan determinar cuál es el nivel de riesgo propio de cada conductor mediante la recolección de varias de sus características personales.¹⁸⁹

Un estudio del Massachusetts Institute of Technology muestra que, pese a que la tecnología para perfeccionar un vehículo 100% autónomo aún está en desarrollo, la recolección de información relacionada con el conductor será esencial para dicho proceso.¹⁹⁰ Para mejorar algunos elementos de seguridad, es necesario que sensores dentro del vehículo recolecten información sobre sus movimientos corporales y gestos faciales para así detectar, por ejemplo, situaciones en las que el conductor se queda dormido mientras maneja.¹⁹¹

Adicionalmente, las preferencias de cada conductor en cuanto a rutas y la velocidad a la que suele manejar, e inclusive los sistemas de entretenimiento dentro del vehículo, es información que, si bien no es esencial para que el vehículo funcione adecuadamente, será relevante para que los consumidores tengan una experiencia más o menos satisfactoria al ser transportados.¹⁹²

¹⁸⁹ Chelsey Colbert, “*Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles*”, Universidad de Stanford, 8, marzo de 2018, <https://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/47/2018/02/Privacy-Under-the-Hood-Towards-an-International-Data-Privacy-Framework-for-Autonomous-Vehicles.pdf>

¹⁹⁰ Lex Fridman, Daniel E. Brown, Michael Glazer, William Angell, Spencer Dodd, Benedikt Jenik, Jack Terwilliger, Aleksandr Patsekin, Julia Kindelsberger, Li Ding, Sean Seaman, Alea Mehler, Andrew Sipperley, Anthony Pettinato, Bobbie Seppelt, Linda Angell, Bruce Mehler, Bryan Reimer, “*MIT Autonomous Vehicle Technology Study: Large Scale Deep Learning Based analysis of Driver Behaviour and Interaction with Automation*”, Massachusetts Institute of Technology, última publicación del estudio en abril de 2019, <https://hcai.mit.edu/avt/>,

¹⁹¹ Ibid.

¹⁹² Chelsey Colbert, “*Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles*”, Universidad de Stanford, 8, marzo de 2018, <https://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/47/2018/02/Privacy-Under-the-Hood-Towards-an-International-Data-Privacy-Framework-for-Autonomous-Vehicles.pdf>, “*Infotainment systems in the vehicle, which offer information, like navigation, or entertainment, like music, is a perk for those in the vehicle and will be promoted to increase consumer adoption of connected capabilities.*”

Se debe considerar que, sin esta clase de información, sería más difícil que los sistemas se adaptaran a las necesidades de los consumidores, pues cada uno cuenta con preferencias distintas al momento de manejar, y éstas influyen en su nivel de satisfacción con el producto, proporcionando un mayor beneficio para el consumidor.¹⁹³

La toma de decisiones individuales automatizadas tiene también un papel importante en el campo de la investigación médica.¹⁹⁴ En vista de que los diagnósticos médicos son actividades altamente complejas, en las cuales cualquier error puede tener repercusiones serias para un paciente, actualmente se desarrollan sistemas de inteligencia artificial que podrían ayudar a diagnosticar pacientes de una manera más precisa.¹⁹⁵

En 2016, tres investigadores contratados por Google LLC¹⁹⁶ publicaron un estudio en el cual desarrollaron un algoritmo autodidacta que puede, por sí mismo, detectar la retinopatía diabética, con un nivel de precisión del 98%.¹⁹⁷ El sistema funciona detectando patrones en información médica obtenida de pacientes que padecen de esta condición.¹⁹⁸ Un algoritmo similar desarrollado por médicos oftalmólogos en Inglaterra, puede predecir más de 50

¹⁹³ Hanna Ballem, “*Comfort in Automated Driving: Analysis of Driving Style Preference in Automated Driving*”, tesis de doctorado, Universidad Técnica de Chemnitz, septiembre 21 de 2017, 67, <http://monarch.qucosa.de/api/qucosa%3A21407/attachment/ATT-0/>, “*As technical realization of highly and fully automated vehicles draws closer, attention is being shifted from sheer feasibility to the question of how an acceptable driving style and thus comfort can be implemented. It is increasingly important to determine, how highly automated vehicles should drive to ensure driving comfort for the now passive drivers.*”

¹⁹⁴ Véronique Barry, Olga Farman, “*The impact of the GDPR on clinical trial research*”, Norton Rose Fulbright, octubre de 2018, <https://www.nortonrosefulbright.com/en/knowledge/publications/9ba711e7/the-impact-of-the%20%20%20%20gdpr-on-clinical-trial-research>

¹⁹⁵ Julia Belluz, “*3 ways AI is already changing medicine*”, marzo de 2019, <https://www.vox.com/science-and-health/2019/3/15/18264314/ai-artificial-intelligence-deep-medicine-health-care>

¹⁹⁶ Mark Bergen, “*Alphabet Finishes Reorganization with New XXVI Company*”, Bloomberg, septiembre de 2017, <https://www.bloomberg.com/news/articles/2017-09-01/alphabet-wraps-up-reorganization-with-a-new-company-called-xxvi>. Su nombre comercial es Google, y hasta 2017 su razón social era Google, Inc. No obstante, con la reorganización de la compañía como una subsidiaria de Alphabet Inc., su razón social es actualmente Google LLC. Actualmente, la compañía está domiciliada en Mountain View, California.

¹⁹⁷ Varun Gulshan, Lily Peng, Marc Coram, “*Development and Validation of Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs*”, Google, Jama Network, diciembre de 2016, <https://jamanetwork.com/journals/jama/fullarticle/2588763>

¹⁹⁸ Ibid.

enfermedades oculares con un nivel de precisión del 94%, e inclusive recomendar el tratamiento adecuado.¹⁹⁹ Otro estudio llevado a cabo por miembros del Centro de Endoscopia del Hospital de Sichuan, China, desarrolló un sistema para la detección del cáncer de colon.²⁰⁰ El algoritmo también fue diseñado para aprender a identificar patrones de imágenes de pacientes con señales de pólipos adquiridas durante colonoscopias y endoscopias.²⁰¹

En el campo de la psicología, se desarrollan actualmente sistemas de inteligencia artificial que podrían ayudar a tratar a personas con problemas de ansiedad y depresión.²⁰² La investigación que ha sido llevado a cabo por la Universidad del Sur de California muestra que algunas personas que sufren de estos trastornos pueden ser mucho más abiertas a compartir su información con un sistema de inteligencia artificial.²⁰³ Parte importante es poder procesar y analizar información corporal transmitida por el usuario al momento de comunicarse con el sistema.²⁰⁴ El estudio está financiado por el ejército de los Estados Unidos y al día de hoy muestra resultados positivos en el tratamiento de personas con trastorno de estrés postraumático.²⁰⁵

¹⁹⁹ “Breakthrough in AI technology to improve care for patients”, Moorfields Eye Hospital, agosto de 2018, <https://www.moorfields.nhs.uk/content/breakthrough-ai-technology-improve-care-patients>

²⁰⁰ Pu Wang, Tyler Berzin, Jeremy Romek, Glissen Brown, Shishira Bharadwaj, Aymeric Becq, Xun Xiao, Peixi Liu, Liangping Li, Yan Song, Di Zhang, Yi Li, Guangre Xu, Mengtian Tu, Xiaogang Liu, “Real-time automatic detection system increases colonoscopic polyp and adenoma detection rates: a prospective randomised controlled study”, BMJ, febrero de 2019, <https://gut.bmj.com/content/early/2019/02/27/gutjnl-2018-317500>

²⁰¹ Ibid. Ver figura 1.

²⁰² Tanya Abrams, “Virtual humans inspire patients to open up, USC study suggests”, USC News, julio de 2014, <https://news.usc.edu/65051/patients-are-more-willing-to-confide-in-computers-not-doctors-usc-study-suggests/>

²⁰³ Kien Hoa Ly, Ann-Marie Ly, Gerard Andersson. “A fully automated conversational agent for promoting mental well-being: A pilot RCT using mixed methods”, *Internet Interventions*, 1 no. 10, (2017), 46, <https://www.sciencedirect.com/science/article/pii/S221478291730091X/pdf?md5=302ec6d7b88bbb31ec8f94af10f97d58&pid=1-s2.0-S221478291730091X-main.pdf>, “The current study adds to the body of knowledge regarding both participants’ experience as well as the outcome of interacting with a conversational agent for promoting mental health.”

²⁰⁴ Tanya Abrams, “Virtual humans inspire patients to open up, USC study suggests”, USC News, julio de 2014, <https://news.usc.edu/65051/patients-are-more-willing-to-confide-in-computers-not-doctors-usc-study-suggests/>

²⁰⁵ Ibid.

La misma Comisión Europea ha reconocido los beneficios que estos sistemas pueden traer al consumidor en cuanto a tecnologías que funcionan a partir de Machine-learning:

*“Las aplicaciones como voz a texto y texto a voz pueden ayudar a las personas con discapacidades y simplificar significativamente su vida (ya existe). Las aplicaciones de Machine-learning integradas en productos o que simplemente operan en el fondo de los servicios digitales, ofrecen la posibilidad de **optimizar el uso de la energía, aprovechar los precios bajos (el argumento clásico presentado a favor de los medidores de energía inteligentes) o comparar fácilmente ofertas complejas (mediante herramientas de comparación de precios)**. Potencialmente, pueden aumentar la eficiencia y la sostenibilidad de los dispositivos, por ejemplo, si detectan automáticamente que pueden pasar al modo de ahorro de energía porque nadie está en casa (por ejemplo, aplicaciones de iluminación inteligente). La aplicación también podría, por ejemplo, autoevaluar si ocurren condiciones inseguras y abordarlas adecuadamente antes de que se produzca una consecuencia negativa (por ejemplo, la versión más elaborada de un "modo de seguridad" ya implementado en calderas).*

*Los sistemas de Machine-learning también pueden facilitar y mejorar el trabajo de las organizaciones de consumidores, la investigación y las autoridades reguladoras: la investigación de mercado podría facilitarse y volverse más precisa. **El monitoreo de precios puede realizarse en tiempo real, lo que permite a los consumidores elegir la mejor oferta. Las entidades encargadas de hacer cumplir la ley podrían usar sistemas de autoaprendizaje para detectar automáticamente los términos de los contratos desleales y alertar a los***

consumidores sobre ellos antes de que realicen una compra en línea.”²⁰⁶

(Resaltado fuera del texto original). (Traducción propia).

Teniendo en cuenta los usos prácticos y los posibles usos futuros de tecnologías que integran los sistemas mencionados anteriormente, en la siguiente sección se explicarán algunas de las ventajas que los mismos representan en términos de eficiencia y reducción de costos.

ii) Ventajas de usar sistemas automatizados de toma de decisiones en el tratamiento de Big Data

En su estudio sobre el mercado de datos, la Comisión Europea reconoció la importancia de la innovación en nuevas tecnologías de análisis de Big Data (*Big Data Analytics*) en este mercado.²⁰⁷

En efecto, la Comisión reconoció que la tecnología reduce costos de transacción, permitiendo un intercambio más eficiente de la información trasladada de un responsable a otro.²⁰⁸

Adicionalmente, permite una mayor comunicación entre los agentes, y que los mismos trabajen de manera conjunta para implementar mejores sistemas de seguridad de la información.²⁰⁹ Se

²⁰⁶ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “*Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world*”, mayo de 2018, 8, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf

²⁰⁷ Comisión Europea, Dirección General de Comunicaciones, redes, contenidos y tecnología, “*European Data Market*”, 203, febrero de 2017, https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1

²⁰⁸ Ibid.

²⁰⁹ Comisión Europea, Dirección General de Comunicaciones, redes, contenidos y tecnología, “*European Data Market*”, 203, febrero de 2017, https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1, “*The recent developments of the so called “3rd Platform of computing”52 – internet-centric computing systems exploiting the power and capabilities of four key technology developments (cloud, mobile, social and big data analytics) have significantly accelerated the exchange of electronic data giving birth to the phenomenon of (electronic) data marketplaces. (...) Data marketplace platforms of this kind can respond to a variety of emerging data market needs, by improving the efficiency of the data value chain, reducing transaction costs, providing a*

puede identificar una ventaja para agentes que por sí solos no cuentan con los recursos necesarios para resolver problemas de interoperabilidad o para garantizar el nivel de seguridad en la información exigido, lo cual podría facilitar su entrada al mercado.²¹⁰

La toma de decisiones automatizadas es parte importante de los servicios de análisis de datos (*Big Data Analytics*).²¹¹ A través de tecnologías de uso corporal, como puede ser un reloj inteligente, o a partir de sistemas integrados en hogares inteligentes, se genera información sobre el consumidor que puede ser usada por compañías para mejorar los servicios que ofrece su negocio.²¹² Sin embargo, los volúmenes de información que pueden ser aprovechados son demasiado altos y complejos, por lo que un análisis manual resultaría ineficiente y costoso, sin mencionar propenso a errores.²¹³ Por esta razón, compañías como CA Inc., conocida también por su nombre comercial CA Technologies,²¹⁴ ofrecen servicios de análisis automatizado de datos a empresas, que a pesar de estar aún en desarrollo,²¹⁵ permiten organizar la información recolectada de manera automática, convertirla a un mismo formato y tomar la decisión sobre qué información resulta relevante para el análisis que requiere a cabo la empresa.²¹⁶

platform for sharing and re-using data sets, and solving data interoperability, privacy and security problems on behalf of data holders who may not have the necessary skills.”

²¹⁰ Comisión Europea, Dirección General de Comunicaciones, redes, contenidos y tecnología, “*European Data Market*”, 203, febrero de 2017, https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1

²¹¹ Yann Guernion, “*What can automated data analytics do for you?*”, Ca Technologies, 12 de abril de 2018, <https://www.ca.com/en/blog-automation/what-can-automated-data-analytics-do-for-you.html>, “*Essentially, automated data analytics is automatic decision making based on data – and not just any data, Big Data*”.

²¹² Ibid.

²¹³ Ibid.

²¹⁴ “*Terms for ca.com*”, Ca Technologies, abril de 2015, <https://www.ca.com/us/legal/terms-for-ca-com.html>. La compañía está actualmente domiciliada en Nueva York, Estados Unidos. A partir de 2018, es una subsidiaria de Broadcom Inc.

²¹⁵ Joel Shapiro, “*Analytics Meets Decision Making: What does Automation Mean for the Future of Data Scientists?*”, Transforming Data With Intelligence, octubre 31 de 2016, <https://tdwi.org/articles/2016/10/31/what-automation-means-for-data-scientist-future.aspx>.

²¹⁶ Yann Guernion, “*What can automated data analytics do for you?*”, Ca technologies, 12 de abril de 2018, <https://www.ca.com/en/blog-automation/what-can-automated-data-analytics-do-for-you.html>

Se entiende entonces que resultaría excesivamente costoso e ineficiente acudir al tratamiento manual de información. Puede entenderse también, que parte integral de los servicios análisis de Big Data implican la toma de decisiones automatizadas en los términos del Reglamento.²¹⁷

Por otro lado, al tratarse de información “*identificable*”, como bien puede ocurrir con la información que recibe un reloj inteligente, un hogar inteligente, un vehículo autónomo, o la información requerida en un estudio médico, podrían entenderse que dentro del Big Data recolectado pueden existir datos personales, en la forma en que los describe el reglamento.²¹⁸

Considerando lo anterior, se procederá a analizar los posibles efectos sobre estos sistemas que trae consigo la restricción del artículo 22, y como esto puede generar un impacto en la libre competencia económica.

iii) Efectos del Artículo 22 en materia de libre competencia económica

En esta sección, se procederá a analizar los efectos que tiene la restricción en el uso de sistemas de toma de decisiones automatizadas en la libre competencia económica. Para estos efectos, se hablará sobre la restricción como un posible desincentivo para la innovación en nuevas tecnologías, la imposición de barreras de entrada al mercado y la mayor concentración en el mercado de datos.

²¹⁷ Reglamento, Art. 22, Num. 1.

²¹⁸ Reglamento, Art. 4, Num. 1, “*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.*”

a. Posibles desincentivos para la innovación en nuevas tecnologías

La libre competencia económica trae consigo el concepto de *eficiencia dinámica*, en virtud del cual los agentes de un mercado se obligan a innovar y a fomentar cambios en la tecnología.²¹⁹ Igualmente, a través de la libre competencia se obliga a los agentes a ofrecer un mejor producto que aquel que ofrecen sus rivales, lo cual incentiva el bienestar de los consumidores.²²⁰ Por esto, el beneficio de los consumidores depende en gran medida de una serie de factores dentro de los cuales están el precio del producto o servicio, la calidad del bien, la variedad de bienes o servicios ofrecidos y la innovación.²²¹

A continuación, se presentan algunos casos en los cuales la prohibición del artículo 22 del Reglamento podría estar generando atrasos, o desincentivando la innovación en las tecnologías de toma de decisiones automatizadas, bajo estudio.

Frente al desarrollo de tecnologías en investigación y diagnóstico médico, así como el tratamiento psicológico de pacientes a partir de algoritmos autodidactas, en primer lugar es importante tener en cuenta que existe una discusión respecto del consentimiento que las personas pueden brindar en los términos del Reglamento.²²²

Si bien el consentimiento del interesado es fundamento legal para la toma de decisiones automatizadas con base en la información que sobre este tiene el responsable del tratamiento,²²³

²¹⁹ Organización para la Cooperación y el Desarrollo Económicos, “*Glossary of Industrial Organization Economics and Competition Law*”, junio de 2002, 82, <http://www.oecd.org/dataoecd/8/61/2376087.pdf>

²²⁰ International Competition Network, “*ICN Merger Guidelines Workbook*”, abril de 2006, 6, <http://old.internationalcompetitionnetwork.org/uploads/library/doc321.pdf>

²²¹ Ibid.

²²² Menno Mostert, Annelien Bredenoord, Monique Biesart, Johannes Van Delden, “*Big Data in medical research and EU data protection law: challenges to the consent or anonymize approach*”, *European Journal of Human Genetics*, 24 no. 7, (2016), 956-960, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5070890/>

²²³ Reglamento, Art. 22, num 2, lit. c.

el artículo 22 no establece de manera expresa cuál es la naturaleza de dicho consentimiento.²²⁴ Aún cuando el artículo 4 del Reglamento establece que el consentimiento es “*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*”,²²⁵ no es muy claro cuáles son las limitaciones de aquel consentimiento, o si el mismo es suficiente para que los datos del interesado sean reutilizados.

Debe tenerse en cuenta que el tratamiento de datos de un paciente, en la práctica, puede ser requerido en más de una ocasión, en especial si se llevan a cabo investigaciones con base en su información.²²⁶ Como ya se ha mencionado, la última etapa en la cadena de valor de los mercados de datos puede incluir tanto el uso como la reutilización de los datos,²²⁷ por lo que dicha práctica no debe ser considerada como poco común.

El debate se extiende a si es suficiente un “*consentimiento general*” o si por cada una de las veces en que hay una decisión con base en el tratamiento de información personal es necesario que el interesado preste su consentimiento.²²⁸ Como se explicaba anteriormente, en la Guía del Grupo de Trabajo de la Comisión Europea, se explica que el consentimiento debe ser “explícito” y que adicionalmente el interesado debe comprender perfectamente lo que está consintiendo.²²⁹

²²⁴ Reglamento, Artículo 22, Num.2.c.

²²⁵ Reglamento, Artículo 4, Num, 11.

²²⁶ Menno Mostert, Annelien Bredenoord, Monique Biesart, Johannes Van Delden, “*Big Data in medical research and EU data protection law: challenges to the consent or anonymize approach*”, *European Journal of Human Genetics*, 24 no. 7, (2016), 956-960, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5070890/>, “*Some suggest that justifications for broad consent models remain contested in the bioethical literature, and they emphasise that these models are insufficient to ensure meaningful individual control over personal data or human samples. Also, it is indicated that, effectively, broad consent is ‘consent for governance’ by certain institutions. Others argue that broad consent is an ethically sound alternative for specific consent, although individuals are not given specific information about future research projects.*”

²²⁷ Ver Capítulo 2, Sección iv: *Noción de datos personales como un mercado.*

²²⁸ *Ibid.*

²²⁹ Ver Capítulo 3, Sección iii, Subsección d: *Excepciones a la restricción.*

Frente lo anterior, es claro que, si se trata de un consentimiento general, a los interesados se les impondría la carga de conocer y objetar la toma de decisiones futuras con base en su información, en caso de no estar de acuerdo con el tratamiento futuro. Por esta razón, sería razonable asumir que muchos de ellos se abstendrían de participar en estos estudios. Por otro lado, si se trata de un consentimiento individual para cada una de las ocasiones en que se tomara una decisión a partir del tratamiento, el responsable tendría que acudir a los interesados, solicitar su consentimiento y esperar su consentimiento. Al respecto, Mosert, Bredenoord, Biesart y van Delden, en un artículo de la Revista Europea de Genética Humana explican:

*“(…) Por un lado, se cuestiona si se puede obtener un consentimiento significativo o legalmente válido (específico, explícito, otorgado e informado libremente) en el momento en que se hace la recopilación de datos, ya que puede que no sea posible prever o comprender las posibles consecuencias prestar el consentimiento. **Por otro lado, se sugiere que obtener el consentimiento específico para cada vinculación o reutilización puede ser casi imposible, porque esto podría resultar en procedimientos costosos y que consumen mucho tiempo, reclutamiento deficiente, sesgo de consentimiento o intrusión injustificada en la vida privada de las personas.**”²³⁰ (Resaltado por fuera del texto original).*

Es en este sentido que, independientemente de la interpretación que pueda hacerse del consentimiento, como general o individual para cada situación, bajo las normas del Reglamento, los procedimientos que involucran algoritmos autodidactas capaces de tomar decisiones, como aquellos capaces de emitir diagnósticos y formular recomendaciones, podrían enfrentarse a serios atrasos ya que, como se evidencia, parte esencial de su desarrollo implica la toma de decisiones automatizadas con base en datos personales, y en ocasiones, su reutilización.²³¹

²³⁰ Ibid., Párrafo 9.

²³¹ Ibid.

Por otro lado, es posible que el mercado de vehículos autónomos y semi-autónomos, del que hacen parte empresas usuarias de datos, también se vea afectado.²³² En el estudio de MIT mencionado anteriormente,²³³ se evidencia que varios elementos de seguridad de estos vehículos requieren del desarrollo de nuevas tecnologías para las cuales es necesaria la recolección y el análisis de una serie de características del conductor al momento de manejar.²³⁴ Es también importante resaltar que el tratamiento y análisis de la información no podría hacerse de manera manual, pues la información recogida involucra a 122 participantes y alrededor de 7.000.000.000 de imágenes corporales de los mismos que deben ser tratadas y analizadas.²³⁵ Tratándose de imágenes que incluyen el rostro de las personas, podría entenderse también como *información sobre una persona física identificada o identificable*.²³⁶

Desde otra perspectiva, el estudio de ciertos patrones comportamentales del conductor y pasajeros, como se mencionaba anteriormente, pueden ser claves para hacer a los vehículos más competitivos en el mercado en la medida en que proveen mayor adaptabilidad del

²³² Alex Davies, “Dont Overestimate the “Semi” in Semiautonomous Cars”, Wired, mayo de 2019, <https://www.wired.com/story/dont-overestimate-semi-semi-autonomous-cars/>. Existen vehículos semiautónomos en diferentes niveles, dependiendo del nivel de autonomía que alcance. Son, en general, vehículos que, si bien cuentan con un mayor grado de autonomía debido a sistemas de apoyo como piloto automático, Super Cruise, Jam Pilot etc., que son ofrecidos desde hace varios años por fabricantes de automóviles de alta gama como Tesla, Cadillac, BMW, Jaguar, Mercedes Benz.

²³³ Lex Fridman, Daniel E. Brown, Michael Glazer, William Angell, Spencer Dodd, Benedikt Jenik, Jack Terwilliger, Aleksandr Patsekin, Julia Kindelsberger, Li Ding, Sean Seaman, Alea Mehler, Andrew Sipperley, Anthony Pettinato, Bobbie Seppelt, Linda Angell, Bruce Mehler, Bryan Reimer, “MIT Autonomous Vehicle Technology Study: Large Scale Deep Learning Based analysis of Driver Behaviour and Interaction with Automation”, Massachusetts Institute of Technology, última actualización abril de 2019, <https://hcai.mit.edu/avt/>

²³⁴ Ibid.

²³⁵ Ibid.

²³⁶ Reglamento, Artículo 4, Num, 1.

automóvil a los gustos de los consumidores.²³⁷ También podría llegar a entenderse como datos personales en los términos del Reglamento.²³⁸

Las tecnologías de *Big Data Analytics* pueden verse también seriamente atrasadas debido a la función que tienen en estas la toma de decisiones automatizadas con base en información que potencialmente puede ser vinculada a un individuo.²³⁹ Esto incluiría tanto a compañías usuarias como a compañías de datos.

Teniendo en cuenta lo anterior, es posible concluir que existe un potencial riesgo para el desarrollo de las tecnologías de tratamiento de datos en varios sectores de la economía a raíz de la implementación del artículo 22 del Reglamento.

En la medida en que se prohíbe o limita el uso de estas tecnologías, es claro que tanto empresas usuarias como empresas de datos, encargadas de desarrollar estos servicios, se verían impedidas para competir por desarrollar la mejor tecnología de tratamiento y análisis. Resulta lógico también considerar que estas se expondrían a muy altos riesgos por incumplir las normas del Reglamento, y podrían ser muy pocos los agentes dispuestos a arriesgarse a ser sancionados.²⁴⁰

²³⁷ Hanna Ballem, “*Comfort in Automated Driving: Analysis of Driving Style Preference in Automated Driving*”, tesis de doctorado, Universidad Técnica de Chemnitz, septiembre 21 de 2017, 67, <http://monarch.qucosa.de/api/qucosa%3A21407/attachment/ATT-0/>, “*As technical realization of highly and fully automated vehicles draws closer, attention is being shifted from sheer feasibility to the question of how an acceptable driving style and thus comfort can be implemented. It is increasingly important to determine, how highly automated vehicles should drive to ensure driving comfort for the now passive drivers.*”

²³⁸ Reglamento, Artículo 4, Num, 1.

²³⁹ Yann Guernion, “*What can automated data analytics do for you?*”, Ca Technologies, 12 de abril de 2018, <https://www.ca.com/en/blog-automation/what-can-automated-data-analytics-do-for-you.html>

²⁴⁰ Reglamento, Art. 83. Las sanciones pueden ser equivalentes a 20.000.000 de euros para el infractor, o mayores.

b. Barreras de entrada al mercado

En esta sección, se discutirán las razones por las que el Reglamento podría ser fuente de barreras de entrada al mercado. Posteriormente, se explicará por que las barreras de entrada deben ser consideradas como barreras de tipo legal. Finalmente, se hará una breve mención sobre la importancia del concepto de abogacía de la competencia y las razones por las que Comisión debió haber analizado a mayor profundidad los posibles efectos anticompetitivos del Reglamento.

Son barreras de entrada aquellos impedimentos que restringen el acceso de un agente a participar en un mercado, o que, de manera similar, retrasan o estancan la entrada de nuevos competidores al mismo.²⁴¹

Dentro de las diferentes clases de barreras de entrada, pueden identificarse las barreras de entrada endógenas y exógenas.²⁴² Las primeras son aquellas que surgen por decisión propia de uno o varios agentes del mercado, como ocurre con estrategias de precios predatorios.²⁴³ Las segundas son aquellas que no surgen por estrategias de los participantes del mercado y, por lo general, no son influenciadas por estos.²⁴⁴ Son también denominadas barreras estructurales, y son impuestas por las condiciones propias del mercado, como son los costos de producción y la demanda.²⁴⁵

²⁴¹ Ibid.

²⁴² Comisión Europea, Centro Común de Investigación, “*Entry barriers and their macroeconomic impact in the EU: an assesment using Quest IIP*”, C. Benedetti-Fasil, M. Sanchez-Martínez, P. Christensen, N. Robledo-Böttcher, 2017, 7, <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108932/kjna2887enn.pdf>

²⁴³ Ibid.

²⁴⁴ Ibid.

²⁴⁵ Ibid.

Dentro de las barreras de entrada de carácter exógeno, pueden también clasificarse aquellas que tienen origen regulatorio o legal. En Colombia, la Superintendencia de Industria y Comercio ha reconocido la existencia de barreras de entrada de esta clase:

*“Dentro de las barreras de entrada que se presentan con mayor frecuencia y por lo tanto, son objeto de análisis se encuentran: **(i) Barreras legales y estructurales;** (ii) Tamaño de los Costos Hundidos; (iii) Tiempo de Entrada; (iv) Escala de Entrada; (v) Identidad de marca, (vi) Requerimientos técnicos e inversión en capital; (vii) Costos de transporte; (viii) Acceso a fuentes de abastecimiento.”*²⁴⁶
(Resaltado fuera del texto original).

A nivel doctrinal, también se ha reconocido la existencia de barreras de entrada de origen legal en sectores regulados de la economía. Tal fue el caso del sector del transporte aéreo de pasajeros en el siglo XX:

*“Históricamente el transporte aéreo de pasajeros se ha caracterizado por estar sujeto a una pesada regulación estatal. En efecto, durante las primeras seis décadas de su de su prestación, en la mayoría de los países desarrollados, los gobiernos aplicaron una estricta regulación en todos los aspectos de la prestación de servicio, una fuerte política de subsidios y **diferentes barreras de entrada de origen legal que restringían la competencia en el mercado.** Según los profesores Borenstein y Rose, como consecuencia de las políticas aplicadas, “los precios eran establecidos conjuntamente por las aerolíneas bajo los auspicios de la International Air Transport Association (IATA), sujetos a la aprobación de la*

²⁴⁶Superintendencia de Industria y Comercio, Colombia, Resolución 40912, junio de 2012, 32.

respectiva autoridad nacional.” Los resultados de estas políticas en Estados Unidos fueron tarifas altas e ineficiente prestación de servicios.”²⁴⁷ (Resaltado fuera del texto original).

Se entienden entonces, como barreras que tienen su origen en una autoridad legislativa o regulatoria, que restringen o hacen muy difícil el acceso de potenciales competidores, y que pueden mantenerse por varios años, incluso décadas.²⁴⁸

Se puede entender también que son barreras que pueden producir efectos nocivos para los consumidores, como precios más altos.²⁴⁹ Al respecto, Dominick Armentano, economista del Instituto Ludwig von Mises para la Escuela Económica Austriaca, escribió lo siguiente:

“Cualquier análisis de los problemas debe distinguir las barreras legales de las barreras económicas. Las discusiones actuales entremezclan ambos conceptos produciendo una confusión generalizada. Las barreras verdaderamente dañinas son las restricciones legales que impiden a las empresas ingresar a los mercados y competir. Por ejemplo, los gobiernos locales pueden restringir la entrada al servicio telefónico local, y pueden limitar la competencia en la televisión por cable y la entrega de basura mediante la concesión de licencias a las empresas seleccionadas y excluyendo a otras. El gobierno federal excluyó legalmente toda entrada en los principales mercados de servicios de transporte aéreo entre 1938 y

²⁴⁷ Alfonso Miranda, Juan David Gutiérrez, “El Derecho de la Competencia en el Sector Aeronáutico Colombiano”, *Revista de derecho de la competencia*, 4 no. 4, (2008): 305, <https://centrocedec.files.wordpress.com/2010/06/6-miranda-y-gutierrez.pdf>, citando a Severin Borstein, Nancy Rose, “How Airlines Markets Work...or Do They? Regulation Reform in the Airline Industry”, *NBER Working Papers 13452*, 2007, 1-2.

²⁴⁸ Ibid.

²⁴⁹ Dominick Armentano, “Barriers to entry”, Ludwig von Mises Institute for Austrian Economics, septiembre de 2000, <https://mises.org/library/barriers-entry>

1978 y actualmente excluye a las empresas privadas de la entrega de correo de primera clase. **Los economistas son casi unánimes en que estas exclusiones regulatorias restringen el comercio y dañan a los consumidores (...) las barreras legales de ingreso al mercado le hacen “corto circuito” al proceso competitivo y dejan a los consumidores con menos opciones o menos bienestar. Las barreras legales protegen las ineficiencias y los márgenes de ganancia de los proveedores existentes, que es probablemente la razón por la que existen en primer lugar.**²⁵⁰

(Resaltado fuera del texto original). (Traducción propia).

La OCDE ha mantenido que la imposición de barreras de entrada a un mercado puede ser dañinas para la libre competencia, incluso cuando las mismas tienen un origen legal o regulatorio.²⁵¹ En efecto, en una publicación de la revista OECD Observer, la Organización estableció lo siguiente:

*Algunas agencias de competencia han adoptado proactivamente el objetivo de las barreras de entrada que fueron creadas innecesariamente por la regulación gubernamental. Lo han hecho mediante la publicación de informes que estudian los efectos de las regulaciones sobre la competencia, identifican alternativas menos restrictivas y abogan por cambios apropiados. **En los sectores regulados, los procedimientos de concesión de licencias, las restricciones territoriales, las normas de seguridad y otros requisitos legales pueden disuadir o retrasar innecesariamente la entrada.** En algunos casos, estas regulaciones parecen ser el*

²⁵⁰ Ibid.

²⁵¹ Organización para la Cooperación y el Desarrollo Económicos, Comité de Competencia, “Barriers to entry”, Mesa redonda sobre política económica, octubre de 2005, 25, <https://www.oecd.org/daf/competition/abuse/36344429.pdf>: “However, sometimes competition is harmed by legal barriers to entry that cannot be justified even on grounds outside of competition policy. Such laws are very attractive targets for the advocacy initiatives of competition agencies.”

*resultado de los esfuerzos de cabildeo por parte de las empresas establecidas para proteger sus negocios. En otros casos, los incumbentes encuentran la manera de aprovechar las regulaciones complejas existentes para impedir la entrada, por ejemplo, al usar las regulaciones como la base de los litigios contra las empresas que buscan entrar.”*²⁵² (Resaltado fuera del texto original). (Traducción propia).

Lo expuesto anteriormente evidencia el fuerte impacto que puede llegar a tener la imposición de medidas regulatorias sobre los mercados y sobre la competencia. Como explican Miranda y Gutiérrez, las barreras de entrada de origen legal pueden generar la prestación de servicios ineficientes por varios años, inclusive décadas.²⁵³ Armentano menciona las ineficiencias que generan en los mercados las barreras regulatorias, exponiendo también un daño a los consumidores en la medida en que se les priva de un mayor bienestar.²⁵⁴

La prohibición del artículo 22 del Reglamento no es ajena a estos problemas. Las nuevas empresas que busquen participar en actividades relacionadas con el análisis y tratamiento de datos personales, podrían verse forzadas a contratar personal adicional que intervengan en la toma de decisiones automatizadas, y que sea suficiente para poder manejar muy altos volúmenes de información.²⁵⁵

²⁵² Organización para la Cooperación y el Desarrollo Económicos, Comité de Competencia, “*Competition and Barriers to Entry*”, enero de 2007, 4, <https://www.oecd.org/competition/mergers/37921908.pdf>

²⁵³ Alfonso Miranda, Juan David Gutiérrez, “El Derecho de la Competencia en el Sector Aeronáutico Colombiano”, *Revista de derecho de la competencia*, 4 no. 4, (2008): 305, <https://centrocedec.files.wordpress.com/2010/06/6-miranda-y-gutierrez.pdf>, citando a Severin Borstein, Nancy Rose, “How Airlines Markets Work...or Do They? Regulation Reform in the Airline Industry”, *NBER Working Papers 13452*, 2007, 1-2.

²⁵⁴ Dominick Armentano, “*Barriers to entry*”, Ludwig von Mises Institute for Austrian Economics, septiembre de 2000, <https://mises.org/library/barriers-entry>

²⁵⁵ Lex Fridman, Daniel E. Brown, Michael Glazer, William Angell, Spencer Dodd, Benedikt Jenik, Jack Terwilliger, Aleksandr Patsekin, Julia Kindelsberger, Li Ding, Sean Seaman, Alea Mehler, Andrew Sipperley, Anthony Pettinato, Bobbie Seppelt, Linda Angell, Bruce Mehler, Bryan Reimer, “*MIT Autonomous Vehicle Technology Study: Large Scale Deep Learning Based analysis of Driver Behaviour and Interaction with Automation*”, Massachusetts Institute of Technology, última publicación en abril de 2019, <https://hcai.mit.edu/avt/>, Las cifras de pueden implicar millones de análisis individuales para estudios comportamentales como el de los vehículos autónomos.

Un artículo publicado por la revista Forbes muestra cómo, días antes de la entrada en vigencia del Reglamento, varias compañías clasificadas en el ranking de Fortune 500 habían tenido que invertir miles de millones de dólares en programas de cumplimiento.²⁵⁶ Muestra también como los pequeños emprendedores se veían impedidos para superar la barrera impuesta por los costos de cumplimiento del Reglamento y por la falta de comprensión del mismo.²⁵⁷ El costo que representa cumplir con el Reglamento, específicamente el artículo 22, es elevado, pero también lo es el costo de incumplir.²⁵⁸ Lo anterior puede llevar a que los potenciales competidores enfrenten barreras de entrada al mercado que no estén en capacidades de superar, por los que serían muy pocos los nuevos emprendedores de la industria de servicios como los de *Big Data Analytics*, o de las tecnologías que hacen uso de la inteligencia artificial.

Considerado lo anterior, para efectos del presente trabajo de investigación, se encuentra que el artículo 22 del Reglamento General de Protección de Datos podría estar generando barreras de entrada de carácter legal. Esto se explica por las razones señaladas a continuación:

En la medida en que el artículo 22 del Reglamento no permite que una decisión se base exclusivamente en el tratamiento automatizado de datos personales, sería necesario contratar mano de obra adicional que se encargue de supervisar los procesos. Debido a que los volúmenes

²⁵⁶ Chris Albert Denhart, “New European Union Data Law GDPR Impacts Are Felt By Largest Companies: Google, Facebook”, *Revista Forbes*, mayo 25 de 2018, <https://www.forbes.com/sites/chrisdenhart/2018/05/25/new-european-union-data-law-gdpr-impacts-are-felt-by-largest-companies-google-facebook/#4b57c3414d36>

²⁵⁷ Ibid.

²⁵⁸ Aysem Diker Vanberg, Mehmet Bilal Ünver, “The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?”, *European Journal of Law and Technology*, 8 no. 1 (2017): 4, <http://ejlt.org/article/view/546/727>: “It must be noted that complying with the GDPR should not to be taken lightly due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 per cent of the total worldwide annual turnover of the preceding year, whichever is greater (...)

de información son demasiado altos y complejos, un análisis manual, o que de cualquier manera involucre expertos en tratamiento de datos, requeriría de una gran cantidad de trabajadores adicionales, haciendo del proceso mucho más costoso. En este sentido, a raíz de las normas impuestas en el Reglamento, se podría estar impidiendo la entrada de empresas que no cuenten con los recursos suficientes para participar en los mercados que involucren sistemas de toma de decisiones automatizadas a partir del tratamiento de datos personales.

Si bien el Reglamento tiene como fin la protección de los derechos de los interesados, no debe ignorarse que el mismo lo hace a partir de una serie de obligaciones que se les imponen a los responsables del tratamiento. El Grupo de Trabajo ha sido claro en que el mismo debe leerse como una *prohibición* de tomar decisiones con base únicamente en el tratamiento de datos personales que puedan afectar a los interesados. En la medida en que la consecuencia de dicha prohibición implica un incremento en los costos, el origen de estas barreras es el artículo contenido en el Reglamento y no las condiciones propias del mercado. Por esta razón, las barreras señaladas en estas secciones son de carácter legal.

Parte importante de este trabajo implica también considerar el concepto de abogacía de la competencia. Este concepto acoge todas aquellas actividades llevadas a cabo por una autoridad de libre competencia, dirigidas a la promoción de un entorno competitivo a través de mecanismos distintos a la exigencia de cumplimiento de la ley, creando consciencia sobre los beneficios de la competencia en el mercado, y usualmente involucrando la interacción con otras autoridades.²⁵⁹

²⁵⁹ International Competition Network, Advocacy Working Group, “*Advocacy and Competition*”, no hay fecha, <https://www.internationalcompetitionnetwork.org/working-groups/advocacy/>

En el caso de la Unión Europea, la máxima autoridad de libre competencia es la Comisión.²⁶⁰ Si bien el Grupo de Trabajo del Artículo 29 considera que el Reglamento genera efectos pro-competitivos entre responsables del tratamiento,²⁶¹ pareciera que en ningún momento la autoridad consideró que también existen posibles efectos anticompetitivos. La Dirección de Competencia no parece haber informado a las autoridades responsables de su redacción y promulgación sobre los posibles atrasos de atrasos en los desarrollos tecnológicos, e imposición de barreras de entrada al mercado. Tampoco parece haberlo hecho respecto de un posible efecto de mayor concentración en los mercados de datos. A continuación, se presentará un análisis respecto de este último punto.

c. Mayor concentración en el mercado de datos

En esta sección, se explicará como el artículo 22 del Reglamento General de Protección de Datos podría tener como efecto una mayor concentración en las etapas de tratamiento y análisis de la cadena de valor del mercado de datos. Para ello, se explicará cuál es, en términos generales, el parámetro empleado para medir la participación de una empresa en el mercado de datos. También, se expondrán las posiciones de dos expertos en tecnologías de la información y del Grupo de Consulta del Consumidor Europeo para explicar cómo podría darse la concentración.

²⁶⁰ “Dirección General de Competencia” Comisión Europea, no hay fecha, http://ec.europa.eu/dgs/competition/index_es.htm

²⁶¹ Comisión Europea, Grupo de Trabajo del Artículo 29, “Directrices sobre el derecho a la portabilidad de datos del Reglamento 2016/679”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 24, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233, “Puesto que permite la transmisión directa de datos personales de un responsable del tratamiento a otro, el derecho a la portabilidad de los datos es también una herramienta importante que respaldará la libre circulación de datos personales en la UE y promoverá la competencia entre los responsables del tratamiento. Facilitará el cambio entre distintos proveedores de servicios y, por lo tanto, promoverá el desarrollo de nuevos servicios en el contexto de la estrategia para el mercado único digital”

Primero, debe aclararse que existe actualmente un debate sobre la relación entre el volumen de datos almacenados por una empresa y su participación en este mercado.²⁶² Si bien hay quienes consideran que el sólo hecho de contar con mayores volúmenes de datos implica *per se* tener una mayor participación, existe una posición contraria, según la cual es igualmente importante contar con los recursos necesarios para sacar información y conocimiento útiles de los datos, y así agregar valor a los mismos.²⁶³

Bajo esta posición, factores como (i) la calidad de los datos, (ii) su relevancia conforme al uso final que se les vaya a dar, (iii) la calidad de las bases de datos construidas y (iv) los algoritmos empleados en el proceso de tratamiento, son factores que ayudan a determinar la participación real de una empresa en el mercado y su poder en éste.²⁶⁴ En este sentido, se opone a la fórmula “*mayor volumen de datos = mayor participación en el mercado/mayor poder de mercado*”.²⁶⁵ Esta posición es compartida por el profesor Torsten Körber de las cátedras de Derecho de la Competencia y Derecho de la Economía Digital en la Universidad de Colonia, Alemania.²⁶⁶

Éste será el parámetro empleado en la presente sección para determinar la participación de las empresas en las distintas etapas de la cadena de valor del mercado de datos.

Teniendo en cuenta lo anterior, se procederá a explicar distintas posiciones que apoyan la teoría de que el Reglamento General de Protección de Datos puede generar una mayor concentración en ciertas etapas de la cadena de valor de este mercado.

²⁶² Torsten Körber, “*Data, Platforms and Competition Law*”, Comisión Europea, 19 de diciembre de 2018, http://ec.europa.eu/competition/information/digitisation_2018/media_en.html

²⁶³ Ibid.

²⁶⁴ Ibid.

²⁶⁵ Ibid.

²⁶⁶ “*Chair of Civil Law, Antitrust and Regulatory Law, Digital Economy Law*”, Universidad de Colonia, 16 de julio de 2019, <http://www.koerber.jura.uni-koeln.de/>

Lothar Determann, abogado especializado en las áreas de protección de datos personales y tecnologías de la información, actualmente socio de la firma Baker McKenzie en las oficinas de Palo Alto, California,²⁶⁷ dictó una conferencia en Bogotá en enero de 2019, en la que habló de las implicaciones prácticas que podría llegar a tener el Reglamento General de Protección de Datos de la Unión Europea en el derecho de la competencia.

Según Determann, uno de los grandes problemas que trae consigo el Reglamento tiene que ver con que las compañías podrían empezar a volverse muy reacias a compartir con otras los datos que tienen almacenados. Esto se debe al alto nivel de requisitos exigidos para poder transferir la información de un responsable del tratamiento a otro, también al alto costo de incumplimiento.²⁶⁸ En su opinión, el efecto inmediato será que las grandes compañías de los mercados de datos tendrán mayor éxito en el desarrollo de tecnologías de inteligencia artificial, pues tienen mayores posibilidades de tener acceso a los “*buenos datos*”, mientras que los start-ups o las compañías más pequeñas tendrán mayores dificultades en tener acceso a datos que les sean útiles. Las segundas se quedarían con los “*datos basura*”.²⁶⁹ Al aplicar el parámetro de participación de mercado explicado, se encuentra que las grandes compañías tendrían mayor

²⁶⁷ “*People: Lothar Determann*”, Baker McKenzie, no hay fecha, <https://www.bakermckenzie.com/en/people/d/determann-lothar>.

²⁶⁸ Lothar Determann, “*Big Data, Economía Naranja y Machine Learning*”, 24 de enero de 2019, conferencia dictada en el 1^{er} Foro del Centro de Estudios en Derecho del Entretenimiento, Tecnología e Información, Pontificia Universidad Javeriana, Bogotá D.C., Colombia. “*The fact that we are restricting companies in terms of sharing data with privacy laws, we are making it so hard for them, they have to get consent, they risk this huge fines and so on, results of course in that companies don’t feel comfortable cooperating and sharing data. Too much risk. Governments also, in some countries, are subjects of privacy laws, and they don’t want to share data with the private sector because they are also worried about backlash under privacy law. Now, what does that do to competition? It means that companies who already have a lot of data will do really well with artificial intelligence, and any start-up companies, the smaller companies that want to get into this space, cannot because they will not get access to good data. They will have to work with this garbage that you have out there, because you won’t get anything good. The Europeans have recognized it as a problem. They don’t really have a solution for it. They now want to take action against the big players and push them by saying that you are abusing your dominance with all this data. But, what should the big players do?*”

²⁶⁹ Ibid.

participación, no por contar con mayores volúmenes de datos, sino por contar con datos de mejor calidad.

Por otro lado, Walter Suárez, médico especializado en informática médica, actual director ejecutivo de estrategias y políticas de tecnología e información en salud de la compañía Kaiser Permanente, planteó su punto de vista frente a esta posibilidad.²⁷⁰ Para Suárez, el efecto que puede llegar a tener el Reglamento a partir de las restricciones impuestas a los sistemas de toma de decisiones automatizadas se podría ver reflejado en la externalización de los servicios de tratamiento y análisis automatizado de datos a un grupo muy selecto de competidores dentro del mercado.²⁷¹

Para Suárez, en efecto, compañías como IBM²⁷², Google LLC y Microsoft Corporation serían los únicos dispuestos a prestar estos servicios, dado que para los demás competidores resulta casi imposible replicar sus capacidades de tratamiento o sus capacidades financieras.²⁷³ Lo anterior tendría como consecuencia un incremento en los precios de estos servicios.²⁷⁴ Conforme al parámetro establecido para determinar la posición de mercado, se observa que bajo la posición de Suárez, serían las compañías con mayores capacidades de tratamiento y análisis de datos en las que se vería reflejada una mayor concentración del mercado.

²⁷⁰ Walter Suárez, entrevista por Santiago Blanco, llamada telefónica, Bogotá, Colombia - Alexandria, VA, Estados Unidos, 6 de junio de 2019, “*En cuanto al artículo 22, los más pequeños podrían verse obligados a acudir a terceros que actuarían como oligopolios: Tienen que acudir a las nubes de Google y de Microsoft y de IBM. Las compañías lo que deben hacer es acudir a los gigantes. Replicar la capacidad de cómputo de estos gigantes es imposible. Las 4 o 5 empresas van a tener a los clientes gigantes y a los clientes pequeños y van a ver que hay un problema. Pueden incrementar los precios.*”

²⁷¹ Ibid.

²⁷² Su razón social es International Business Machines Corporation. Actualmente está domiciliada en Amonok, Nueva York.

²⁷³ Walter Suárez, entrevista por Santiago Blanco, llamada telefónica, Bogotá, Colombia - Alexandria, VA, Estados Unidos, 6 de junio de 2019.

²⁷⁴ Ibid.

Por otro lado, el Grupo de Consulta del Consumidor Europeo estimó que los mercados de sistemas de inteligencia artificial y de toma de decisiones automatizadas pueden ser muy propensos a la concentración desde el punto de vista de la oferta.²⁷⁵ Dicha concentración puede ocurrir en la medida en que varias etapas de la cadena de valor de los datos personales se podrían estar volviendo propensos a concentrarse más verticalmente. Así, el Grupo de Consulta estableció lo siguiente:

“El control que tiene el consumidor sobre las aplicaciones de Machine-learning y los dispositivos IoT²⁷⁶ también está restringido por algunos factores del mercado.

Varias características de los sistemas de inteligencia artificial y sistemas de toma de decisiones automatizadas pueden incrementar las tendencias de concentración en los mercados que están impulsados por estos (...).

Debido a la combinación de hardware, software, y servicios conexos, el riesgo de integración vertical y, como consecuencia, la concentración del mercado es cada vez más generalizada. Como resultado, es más fácil encerrar a los consumidores en los productos de un mismo fabricante o en un ecosistema cerrado que carece de interoperabilidad. De esta forma, los consumidores cuentan con menos opciones, y los precios aumentan debido a que hay menos competencia en el mercado.²⁷⁷ (Resaltado fuera del texto original). (Traducción propia).

²⁷⁵ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world”, mayo de 2018, 10, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf

²⁷⁶ El término se refiere al “Internet de las Cosas”. Corresponde a tecnologías integradas, por ejemplo, en hogares inteligentes, como sistemas de alumbrado automáticos que detectan cuándo una persona usualmente se encuentra en su hogar y cuando no, para así ahorrar energía.

²⁷⁷ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world”, mayo de 2018, 10, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf

Tiene sentido pensar en que la concentración del mercado de datos ocurriría de manera vertical si se tienen en cuenta las actividades que componen la cadena de valor, pues, como ya se ha señalado, una misma compañía puede situarse en distintas etapas de esta misma cadena.²⁷⁸ Una compañía que ya cuenta con bases de datos podría adquirir a otra que preste servicios de tratamiento y análisis de datos. Dicho supuesto es señal de un incremento en su participación de mercado siguiendo el parámetro empleado en esta sección.

Así, hay señales de que empresas como aquellas señaladas por Suárez pueden consolidarse de manera estratégica en más de una de las etapas de la cadena, con mayor facilidad, pues como explica el Grupo de Consulta, son mercados que de por sí, son muy propensos a ello, asumiendo actividades en otras etapas en la cadena.²⁷⁹ Aquí nos referimos tanto a empresas de datos, como a empresas usuarias con el potencial de producir o prestar algunos de los servicios que prestan las empresas de datos.

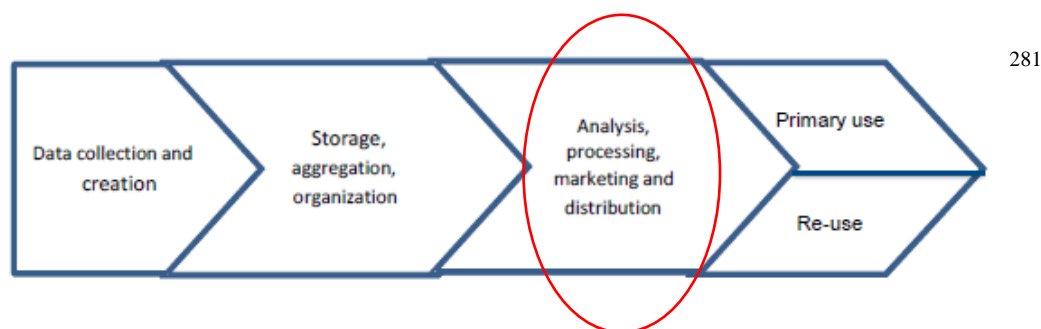
Con base en esto, en la medida en que muchos agentes pequeños pueden optar por exteriorizar los servicios de tratamiento y análisis de datos personales, sea debido a que no puedan contratar personal adicional que intervenga en la toma de decisiones, o debido a que no están dispuestos a asumir los riesgos de incumplimiento,²⁸⁰ serían las grandes compañías quienes podrían entrar

²⁷⁸ Comisión Europea, Dirección General de Comunicaciones, redes, contenidos y tecnología, “*European Data Market*”, 28, febrero de 2017, https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1, (i) Recolección y creación de datos, (ii) almacenamiento, agregación y organización de datos, (iii) análisis, tratamiento, mercadeo y distribución, y (iv) uso y reutilización. Ver el caso de Snowflake, que presta sus servicios en las etapas de almacenamiento y de análisis.

²⁷⁹ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “*Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world*”, mayo de 2018, 10, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf

²⁸⁰ Ibid., Aysem Diker Vanberg, Mehmet Bilal Ünver, “*The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*”, *European Journal of Law and Technology*, 8 no. 1 (2017): 8, <http://ejlt.org/article/view/546/727>, “*It must be noted that complying with the GDPR should not to be taken lightly*

a reemplazarlos, generando así, una mayor concentración en el sector señalado en la siguiente gráfica:



Frente al problema, el Grupo plantea la siguiente recomendación:

*“Al evaluar el abuso del poder de mercado o los efectos de las fusiones y adquisiciones, **deben tenerse más en cuenta los datos o los sistemas de inteligencia artificial de las partes que se integran, ya que podrían utilizarse para aprovechar el poder de mercado de un mercado a otro.** La Comisión Europea debería considerar la introducción de un nuevo criterio en las normas jurisdiccionales del Reglamento de concentraciones de la UE.”²⁸² (Resaltado fuera del texto original). (Traducción propia).*

Si bien una reforma al régimen de control de integraciones puede ser una solución válida, en la que se tienen en cuenta no solo el volumen sino los datos con los que se cuenta y los sistemas de inteligencia artificial empleados, el Grupo es insistente en proponer que deben existir mayores garantías de cumplimiento del Reglamento, ignorando toda posibilidad de que el

due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 per cent of the total worldwide annual turnover of the preceding year, whichever is greater.”

²⁸¹ Comisión Europea, Dirección General de Comunicaciones, redes, contenidos y tecnología, “*European Data Market*”, 28, febrero de 2017, https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1.

Ver “Figure 1: The Data Value Chain and the Data Ecosystem”.

²⁸² Ibid.

mismo podría ser generador de mayor concentración, en un mercado que de por sí ya es propenso a esto:

*“Las autoridades de supervisión apropiadas deben garantizar la correcta aplicación de los artículos 13, 14, 15 y 22 GDPR y garantizar que el uso de algoritmos sea legal y no tome decisiones perjudiciales socialmente no deseadas basadas en información sobre los consumidores.”*²⁸³ (Traducción propia).

5. Toma de decisiones automatizadas y el argumento de la discriminación

En esta sección se hará una consideración final sobre los efectos discriminatorios que se presentan con el uso de algunos sistemas de toma de decisiones automatizadas, explicando como esto se debe a factores externos como la información que es empleada en los procesos de tratamiento, y cómo se propone que la mejor solución no es la limitación a su uso.

Uno de los argumentos en contra del uso de los sistemas de toma de decisiones automatizadas tiene que ver con la discriminación. En efecto, el Grupo de Trabajo del Artículo 29 manifestó que la elaboración de perfiles puede resultar en la perpetuación de estereotipos raciales y formas de segregación social.²⁸⁴ Explicó que puede terminar encasillando a una persona en una categoría específica que lo limite en su libertad de elección a los productos que le son sugeridos, así como negar la prestación de ciertos bienes o servicios como son libros, música o noticias, argumentando que la elaboración de perfiles puede llevar a predicciones inexactas sobre un individuo.²⁸⁵

²⁸³ Ibid.

²⁸⁴ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, Revisadas por última vez por el Grupo el 6 de febrero de 2018, 11, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

²⁸⁵ Ibid.

No obstante, con base en los conceptos planteados a lo largo de este trabajo de investigación, se puede afirmar que no por esto su uso debe ser restringido en la forma en que lo hace el Reglamento, pues existen medidas alternativas que permiten que los sistemas sean mejorados gradualmente.²⁸⁶

El Grupo de Consulta del Consumidor Europeo, argumentó que, en parte, la razón por la que dichos sistemas generaban discriminación era una falta de transparencia en los procesos.²⁸⁷ No obstante, reconoció que en la medida en que las organizaciones sean más abiertas, y exista un financiamiento constante en investigación, sería más fácil corregir estas inconsistencias, permitiendo así la existencia de sistemas de Machine-learning “justos”.²⁸⁸

Recientemente, uno de estos sistemas fue empleado para predecir la posibilidad de que personas que habían sido condenadas por la comisión de un delito, pudiesen reincidir en la comisión otro delito.²⁸⁹ El resultado fue que el sistema atribuyera una mayor posibilidad de reincidencia a ciudadanos afrodescendientes.²⁹⁰ La razón por la que no se pudo determinar las

²⁸⁶ Ann Williams, Catherine Brooks, Yotam Shmargad, “How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications”, *Penn State University Press*, 8 no. 1, (2018), 78-115, https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0078#metadata_info_tab_contents.

²⁸⁷ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world”, mayo de 2018, 10, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf: “Currently, however, automated decision-making processes are highly intransparent, worse, even those designing them regularly publicly refuse to take responsibility for their output. It remains unclear whether results produced by algorithms are merely correlations or based on real causalities. The result can be arbitrary exclusion, discrimination and increasing inequalities. In a connected world driven by artificial intelligence, the output will be actions taken automatically by machine-learning powered devices such as robots or services based on automated decision processes. Responsibility for those actions, need to be clearly attributed and defined.”

²⁸⁸ Ibid., 16, “There must be financial support available for research activities to develop ‘discrimination-aware data processing’ and ‘fair machine-learning’ to prevent unfair decision-making”.

²⁸⁹ Bernard Marr, “Artificial Intelligence has A Problem With Bias, Here’s How to Tackle it”, *Forbes*, enero de 2019, <https://www.forbes.com/sites/bernardmarr/2019/01/29/3-steps-to-tackle-the-problem-of-bias-in-artificial-intelligence/#33ef3877a128>

²⁹⁰ Ibid.

causas de que el algoritmo llegase a estas conclusiones no pudo ser determinado, pues su funcionamiento era cerrado a formas de auditoría externa.²⁹¹

En un estudio realizado por la Agencia de los Derechos Fundamentales de la Unión Europea, se propusieron algunas medidas a través de las cuales se podrían aprovechar los beneficios de los sistemas mencionados, sin que ocurra una vulneración de los derechos de los individuos.²⁹² Esas consisten en: (i) emplear sistemas transparentes, (ii) llevar a cabo evaluaciones de impacto, (iii) verificar la calidad de la información, (iv) asegurarse de que los algoritmos puedan ser explicados y comprendidos.²⁹³

La primera de ellas es coherente con una de las recomendaciones emitidas por el Grupo de Consulta del Consumidor.²⁹⁴ Esta garantiza una mayor libertad en las decisiones tomadas por los consumidores, y permite que el público esté enterado de la forma a través de la cual opera el proceso de la toma de las decisiones.²⁹⁵ Lo anterior también permite que otros contribuyan a detectar y a rectificar las aplicaciones erróneas del sistema.²⁹⁶ Para ello es también necesario que el mismo pueda ser explicado y comprendido, por lo menos de manera general, o por lo

²⁹¹ Ibid.

²⁹² Agencia de los Derechos Fundamentales de la Unión Europea, “#Big Data: Discrimination in Data Supported Decision Making”, no hay fecha, 11, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf. Ver también, Luise Matsakis, “What does a fair algorithm actually look like?”, Wired, noviembre de 2018, <https://www.wired.com/story/what-does-a-fair-algorithm-look-like/>

²⁹³ Ibid.

²⁹⁴ Comisión Europea, Grupo de Consulta del Consumidor Europeo, “Policy recommendations for a safe and secure use of artificial intelligence, automated decision-making, robotics and connected devices in a modern consumer world”, mayo de 2018, 16, https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf: “Some algorithmic decision-making processes must be made transparent to the public to secure free consumer decisions in future and have an informed debate about opportunities, risks and challenges of algorithmic decision-making. Consumers must be given transparency on the logic behind relevant ADM processes, which includes transparency on the data upon which a decision is based and the criteria behind the decision. ADM processes must be made available to peer-to-peer scientific review. This might require either the disclosure of source code or the use of techniques revealing how an ADM process works without disclosing the source code.”

²⁹⁵ Ibid.

²⁹⁶ Agencia de los Derechos Fundamentales de la Unión Europea, “#Big Data: Discrimination in Data Supported Decision Making”, no hay fecha, 11, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf, “Being as transparent as possible: opening up for scrutiny how algorithms were built supports the further development of these tools and allows others to detect, and therefore rectify, any erroneous applications”

menos en cuanto a los fundamentos de las operaciones que están detrás de la decisión.²⁹⁷ El ejercicio de las evaluaciones de impacto permite que se identifique cuáles son los potenciales sesgos en esta materia, e implica la evaluación sobre diferentes clases de discriminación, tales como aquella basada en género, edad, grupo étnico, religión, u orientación sexual o política.”²⁹⁸ Por último, a pesar de que pueda ser la parte más compleja, es necesario verificar la calidad de los datos recolectados y empleados en el proceso para verificar su calidad.²⁹⁹

En un artículo publicado en 2018, Anne Williams, Catherine Brooks y Yotam Shmargad, expusieron el problema, explicando que los algoritmos tienden a discriminar basados en la omisión de información adicional que debería ser incluida en el tratamiento.³⁰⁰ Esto muestra que las causas de estas decisiones no se deben realmente a un problema de los sistemas como tal, sino de la información que se le está siendo proporcionada. En parte, la razón por la que se encuentran sesgos, es porque los sistemas están basados en información que de por sí muestran un patrón de discriminación; los algoritmos toman decisiones basándose en información que refleja discriminación en el mundo real, como se muestra en el siguiente ejemplo:

“En términos muy simplificados, un algoritmo puede elegir a un hombre blanco de mediana edad para llenar una vacante basándose en el hecho de que otros hombres blancos de mediana edad fueron previamente contratados para la misma posición y posteriormente promovidos. Esto sería pasar por alto el hecho de que la razón por la que fue contratado y promovido se debió más al hecho de que es un hombre

²⁹⁷ Ibid., “The challenge of understanding the mathematical background of a statistical method or an algorithm does not prevent a general description of the process and/or rationale behind the calculations feeding the decision making, most notably, which data were used to create the algorithm.”

²⁹⁸ Ibid.

²⁹⁹ Ibid.

³⁰⁰ Ann Williams, Catherine Brooks, Yotam Shmargad, “How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications”, Penn State University Press, 8 no. 1, (2018), 78-115, https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0078#metadata_info_tab_contents.

blanco de mediana edad, en lugar de que era bueno en el trabajo.”³⁰¹ (Traducción propia).

En su artículo, Williams, Brooks y Shamragad proponen que la solución para lograr que los sistemas sean más justos, consiste precisamente en *rectificar* las injusticias que presentan los algoritmos:

“(…) la toma de decisiones algorítmica se basa necesariamente en las correlaciones. Estas relaciones de datos pueden vincular los rasgos, las acciones pasadas, los contactos sociales y las categorías sociales de una persona con personas que tuvieron resultados buenos o malos en el pasado. **Este proceso puede replicar la discriminación pasada o hacer suposiciones sobre un individuo debido a que pertenece a un grupo específico, y puede hacerlo incluso cuando un individuo mantiene los datos privados o cuando se omiten categorías sensibles.** El sistema puede crear distorsiones en las acciones de las personas, ya que favorece ciertas señales, y puede potencialmente aumentar la discriminación. **Los algoritmos pueden hacer predicciones a partir de datos increíblemente complejos, pero en última instancia somos responsables de lo que hacen.** En todas las culturas, contextos, regiones geográficas y sistemas sociotécnicos, los algoritmos deben crearse teniendo en cuenta la imparcialidad. Luego debemos verificar los resultados injustos y actuar para corregir cualquier injusticia algorítmica. **La revisión continua de cómo usamos la toma de decisiones algorítmica y lo que nuestros algoritmos han aprendido a valorar con el tiempo**

³⁰¹ Bernard Marr, “Artificial Intelligence has A Problem With Bias, Here’s How to Tackle it”, Forbes, enero de 2019, <https://www.forbes.com/sites/bernardmarr/2019/01/29/3-steps-to-tackle-the-problem-of-bias-in-artificial-intelligence/#33ef3877a128>

es fundamental para una sociedad justa.³⁰² (Resaltado fuera del texto original).

(Traducción propia).

Con base en lo expuesto, se propone que la solución a los problemas de parcialización y discriminación que aún presentan los sistemas de toma de decisiones a que se refiere este estudio, no debe ser su prohibición o restricción, sino todo lo contrario; su uso a través de la implementación de medidas que permitan mejorar los sistemas, buscando un mayor control sobre la información que es proporcionada a los sistemas, y una mayor transparencia en la forma en que los mismos operan, con tal de que la tecnología pueda ser mejorada gradualmente, ampliando sus campos de aplicación, permitiendo el desarrollo nuevas tecnologías y de mercados emergentes, incentivando a que los agentes puedan competir por desarrollar un mejor producto.

6. Conclusiones

Expuestos los argumentos frente a cada uno de los temas analizados en el trabajo de investigación, se presentarán las siguientes conclusiones generales. Posterior a esto, se procederá a responder la pregunta de investigación.

³⁰² Ibid., 110.

i) Conclusión respecto del análisis histórico en el tratamiento automatizado de datos y antecedentes históricos en materia de normas sobre datos personales

Frente a este punto, se concluye que los sistemas de tratamiento automatizado han sido herramientas de gran utilidad para organizar información y obtener conocimiento a partir de toda clase de datos, incluidos los datos que pueden clasificarse como personales. No obstante, en ocasiones han sido empleados por el Estado en contra de sus propios ciudadanos. En efecto, se encuentra que la experiencia frente algunos regímenes totalitarios europeos del siglo XX ayudaron a moldear una concepción sobre la importancia de la privacidad y el cuidado de la información personal. Por esta razón, se encuentra que la experiencia europea, específicamente la experiencia alemana, es un factor influyente en la adopción de la política de protección de datos actual de la Unión Europea.

ii) Conclusión respecto de los principales elementos que introduce el Reglamento General de Protección de Datos de la Unión Europea

Aunque el Reglamento es una norma enfática en garantizar los derechos de los interesados, las normas que se aplican a los responsables del tratamiento pueden producir efectos adversos en el mercado. Se observa que la forma en que se redacta el *derecho a la portabilidad de datos* puede permitir que los responsables del tratamiento se abstengan de transferir información a otros responsables por petición expresa del interesado. Lo anterior no solo perjudica a los interesados, sino a las empresas que busquen ingresar a los mercados que requieran de la disponibilidad de datos personales para el desarrollo de productos y prestación de servicios específicos.

Respeto del artículo 22 del Reglamento, se concluye que es una norma que contiene varias dificultades interpretativas y términos que pueden considerarse como ambiguos, como el de producir *efectos jurídicos* sobre el interesado, o afectarlo *significativamente*. Son conceptos que se muestran especialmente difíciles de interpretar en el marco de derechos como el de la educación y la *autodeterminación informativa*. Se concluye que al haber incertidumbre sobre cuáles son los escenarios en los que se permite la toma de decisiones y en los que no, es posible que algunas compañías se muestren reacias a participar en actividades que involucren el uso de los sistemas a los que se refiere el artículo, sea para no arriesgarse a una sanción, o sea porque no pueden asumir elevados costos de cumplimiento.

iii) Conclusión respecto de los procesos automatizados de toma de decisiones y *profiling*

De acuerdo a la información presentada en este capítulo, es posible concluir que los procesos automatizados de toma de decisiones son parte integral del desarrollo de nuevas tecnologías en distintos sectores, muchos de los cuales necesariamente funcionan a través de la elaboración de perfiles. Esto se puede evidenciar en los sectores automotriz, médico y de la psicología. Se encuentra que representan un beneficio potencial a futuro para el bienestar del consumidor en cuanto a seguridad vial, detección temprana de enfermedades y tratamiento de desórdenes psicológicos. De manera general, se encuentra también que los sistemas representan ventajas para los procesos de tratamiento de Big Data, ya que pueden hacer del proceso más eficiente y menos costoso de lo que sería acudir a un tratamiento manual de la información.

En la medida en que muchos de sus usos requieren del tratamiento de información que puede ser asociada a una persona natural, mediante la restricción del Reglamento, puede que el

desarrollo de muchas de estas tecnologías se vea limitado. Por ello, existe la posibilidad de que los agentes tengan que acudir a alternativas menos eficientes en materia de tiempo y costos. Esto afectaría tanto a empresas de datos como a empresas usuarias de datos.

iv) Conclusión respecto de los efectos que el artículo 22 del Reglamento General de Protección de Datos tiene sobre la libre competencia económica y respecto del argumento de la discriminación

Considerando todo lo anterior, y conforme a la información expuesta en el capítulo correspondiente, se encuentra que el Reglamento podría representar un riesgo para la libre competencia desde tres perspectivas: (i) puede ser un desincentivo para la innovación en nuevas tecnologías, (ii) podría estar imponiendo barreras de entrada al mercado y (iii) podría estar propiciando una mayor concentración en el mercado de datos.

La toma de decisiones automatizadas a partir del tratamiento de datos personales es parte integral del desarrollo de nuevas tecnologías en sectores como el de los vehículos autónomos, el de la medicina y el de la psicología. No obstante, debates como el de la naturaleza del consentimiento otorgado por el interesado podrían generar incertidumbre sobre la legalidad del tratamiento y toma de decisiones en múltiples escenarios. Se encuentra que lo anterior podría desincentivar significativamente su desarrollo, generando serios atrasos en el desarrollo de tecnologías que representan beneficios para los consumidores. En la medida en que éste se vea limitado, se concluye que tanto empresas de datos como empresas usuarias de datos estarían restringidas para competir por ofrecer el mejor sistema y la mejor tecnología.

El Reglamento podría estar imponiendo barreras de entrada al mercado en la medida en que limita la toma de decisiones automatizadas con base exclusivamente en el tratamiento de datos personales. Lo anterior podría llevar a que muchas empresas se vean obligadas a contratar mano de obra adicional que se encargue de intervenir en cada uno de estos procesos, y en cada una de las decisiones que pueda afectar a los interesados. Debido a los altos volúmenes y la complejidad de la información, un análisis manual, o que de cualquier forma involucre la intervención de expertos en el manejo de datos, requeriría de una gran cantidad de trabajadores adicionales, incrementando así los costos. El Grupo de Trabajo del Artículo 29 estableció que el artículo 22 debe ser leído como una prohibición. En este sentido, se concluye que es a raíz de la prohibición que impone el Reglamento, y no de las condiciones propias del mercado, que se estaría restringiendo la entrada de empresas que no cuentan con los recursos suficientes para participar en mercados que involucren sistemas de toma de decisiones automatizadas con base en el tratamiento de datos personales.

Se concluye también que el Reglamento puede ser fuente de una mayor concentración en el mercado de datos. Debido a los altos costos que representa incumplir el Reglamento, muchas compañías podrían optar por exteriorizar servicios como los de tratamiento y análisis de datos personales a grandes compañías que cuentan con la capacidad financiera y de personal capacitado necesarias. Teniendo en cuenta los parámetros empleados para medir la participación de una empresa en el mercado de datos, se concluye que, efectivamente, el Reglamento puede ser un factor influyente en la mayor concentración de este mercado.

Finalmente, respecto de la discriminación, se encuentra que el problema no surge en los sistemas como tal, sino en la información que les está siendo introducida, por lo que aún hay

lugar a mejorar estas inconsistencias a través de varias alternativas, y la respuesta no debería ser limitar su uso de manera general.

v. Respuesta a la pregunta de investigación

A modo de conclusión, debe hacerse una consideración final. El propósito de este trabajo de investigación no es el de pormenorizar la importancia de la protección de la privacidad y los datos personales, sino el de señalar que a partir de la implementación del Reglamento se podrían estar vulnerando otros valores fundamentales como la eficiencia, el bienestar de los consumidores y la libre competencia. Así como la protección de los datos personales es fundamental para todo interesado, también lo son los valores señalados anteriormente, por lo que su protección debería ser también prioridad para las entidades regulatorias.

En este orden de ideas, teniendo en cuenta las conclusiones presentadas frente a las diferentes problemáticas analizadas, se encuentra que el Reglamento General de Protección de Datos de la Unión Europea es un potencial desincentivo para la innovación en nuevas tecnologías y para el desarrollo de la libre competencia económica en mercados emergentes.

A pesar de que los sistemas de toma de decisiones automatizadas aún se encuentran en una etapa primitiva, y su uso aún puede ser motivo de controversia, existe un amplio potencial a futuro para estos sistemas. Varias medidas pueden ser implementadas para corregir sus inconsistencias y volverlos gradualmente más “justos”. Se debe permitir que los agentes compitan por desarrollar un mejor producto, generando así condiciones de eficiencia y bienestar de los consumidores.

7. Bibliografía

1. “About Snowflake”. Snowflake. No hay fecha. <https://www.snowflake.com/about/>
2. Agencia de los Derechos Fundamentales de la Unión Europea. “#Big Data: Discrimination in Data Supported Decision Making”. No hay fecha. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf
3. Ahmed, Raad. “GDPR: What Small Businesses Need To Know. Forbes. Marzo de 2019. <https://www.forbes.com/sites/theyec/2019/03/04/gdpr-what-small-businesses-need-to-know/#54e94f373197>
4. Armentano, Dominick. “Barriers to entry”. Ludwig von Mises Institute for Austrian Economics. Septiembre de 2000. <https://mises.org/library/barriers-entry>
5. Asamblea General de las Naciones Unidas. Declaración Universal de los Derechos humanos. Diciembre de 1948. <https://www.un.org/es/universal-declaration-human-rights/>
6. Asamblea Legislativa del Reino de Suecia. Ley de Protección de Datos. Mayo 11 de 1978. <http://rkrattsbaser.gov.se/sfst?bet=1973:289>
7. Asamblea Nacional de Francia. Ley 78-17 sobre datos, archivos y libertades. Enero 6 de 1978. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>

8. Atkinson, Paul. "ENIAC versus Colossus and the early presentation of electronic computers". Universidad de Oxford. 2014. http://shura.shu.ac.uk/9501/3/Atkinson_-_Eniac_versus_Colossus_paper_%26_url.pdf
9. "Autonomous Vehicles". Gartner. No hay fecha. <https://www.gartner.com/it-glossary/autonomous-vehicles/>
10. Ballem, Hanna. "Comfort in Automated Driving: Analysis of Driving Style Preference in Automated Driving". Tesis de doctorado. Universidad Técnica de Chemnitz. Septiembre 21 de 2017. <http://monarch.qucosa.de/api/qucosa%3A21407/attachment/ATT-0/>
11. Barry, Véronique. Farman, Olga. "The impact of the GDPR on clinical trial research". Norton Rose Fulbright. Octubre de 2018. <https://www.nortonrosefulbright.com/en/knowledge/publications/9ba711e7/the-impact-of-the%20%20%20%20%20gdpr-on-clinical-trial-research>
12. Belluz, Julia. "3 ways AI is already changing medicine". Vox. Marzo de 2019. <https://www.vox.com/science-and-health/2019/3/15/18264314/ai-artificial-intelligence-deep-medicine-health-care>
13. Bergen, Mark. "Alphabet Finishes Reorganization with New XXVI Company". Bloomberg. Septiembre de 2017. <https://www.bloomberg.com/news/articles/2017-09-01/alphabet-wraps-up-reorganization-with-a-new-company-called-xxvi>.

14. *"Birth of Colossus and Enniac"*. *It-History*. No hay fecha. http://it-history.net/colossus_and_ENIAC.html
15. Black, Edwin. *"IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation"*. (No hay ciudad: Crown Books, 2001.)
16. Borstein, Severin. Rose, Nancy. *"How Airlines Markets Work...or Do They? Regulation Reform in the Airline Industry"*. *NBER Working Papers 13452*, 2007. 1-2.
17. Bradford, Ana. Citada por Waxman, Olivia. *"The GDPR in Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History"*, *Time Magazine*. Mayo 24 de 2018. <http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>
18. *"Breakthrough in AI technology to improve care for patients"*. *Moorfields Eye Hospital*. Agosto de 2018. <https://www.moorfields.nhs.uk/content/breakthrough-ai-technology-improve-care-patients>
19. Brill, Julie. *"GDPR's first anniversary: A year of progress in privacy protection"*. *Microsoft*. Mayo de 2019. <https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/>
20. Burges, Matt. *"What is GDPR? The summary guide to GDPR compliance in the UK"*. *Wired*. Enero de 2019. <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>

21. Chair of Civil Law. *Antitrust and Regulatory Law, Digital Economy Law*". Universidad de Colonia. 16 de julio de 2019. <http://www.koerber.jura.uni-koeln.de/>
22. Colbert, Chelsey. "Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles". Universidad de Stanford. Marzo de 2018. <https://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/47/2018/02/Privacy-Under-the-Hood-Towards-an-International-Data-Privacy-Framework-for-Autonomous-Vehicles.pdf>
23. "Colossus Birth of the Digital Computer". Crypto Museum. No hay fecha. <https://www.cryptomuseum.com/crypto/colossus/index.htm>
24. Comisión Europea. Centro Común de Investigación. "Entry barriers and their macroeconomic impact in the EU: an assesment using Quest III". Benedetti-Fasil, C. Sanchez-Martínez, M. Christensen, P. Robledo-Böttcher, N. 2017. <http://publications.jrc.ec.europa.eu/repository/bitstream/JRC108932/kjna2887enn.pdf>
25. Comisión Europea. Dirección General de Comunicaciones, redes, contenidos y tecnología. "European Data Market". Febrero de 2017. https://sites.google.com/a/open-evidence.com/download/repository/SMART20130063_Final%20Report_030417_2.pdf?attredirects=0&d=1
26. Comisión Europea. Grupo de Consulta del Consumidor Europeo. "Policy recomendations for a safe and secure use of artificial intelligene, automated decision-

- making, robotics and connected devices in a modern consumer world*". Mayo de 2018.
https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf
27. *Comisión Europea. Grupo de Trabajo del Artículo 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Revisadas por última vez por el Grupo el 6 de febrero de 2018.*
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
28. *Consejo de Europa. Convención Europea de Derechos Humanos. 3 de septiembre de 1953. Artículo 8.* https://www.echr.coe.int/Documents/Convention_SPA.pdf
29. *Constitución de Estados Unidos. Artículo 1, Sección 2.*
30. *Cool, Alison. "Europe's Data Protection Law is a Big, Confusing Mess". New York Times. Mayo de 2018.* <https://www.nytimes.com/2018/05/15/opinion/gdpr-europe-data-protection.html>
31. *Da Cruz, Frank. "Herman Hollerith." Columbia University. Última actualización 30 de mayo de 2019. No hay fecha.*
<http://www.columbia.edu/cu/computinghistory/hollerith.html>
32. *"Data is Power: Profiling and Automated Decision-Making in GDPR". Privacy International. 2017.* <https://privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr>

33. *Denhart, Chris Albert. "New European Union Data Law GDPR Impacts Are Felt By Largest Companies: Google, Facebook". Revista Forbes. Mayo 25 de 2018. <https://www.forbes.com/sites/chrisdenhart/2018/05/25/new-european-union-data-law-gdpr-impacts-are-felt-by-largest-companies-google-facebook/#4b57c3414d36>*
34. *Departamento de Comercio de los Estados Unidos. Oficina del Censo. División de Datos de Usuarios. 100 Years of Data Processing, enero de 1991. <https://play.google.com/books/reader?id=uCeu4sHRLfgC&hl=en&pg=GBS.PA4>*
35. *Determann, Lothar. "Big Data, Economía Naranja y Machine Learning". 24 de enero de 2019. Conferencia dictada en el 1er Foro del Centro de Estudios en Derecho del Entretenimiento, Tecnología e Información. Pontificia Universidad Javeriana. Bogotá D.C. Colombia.*
36. *"ENIAC". Engineering and Technology. Última actualización el 23 de noviembre de 2017. <https://ethw.org/ENIAC>*
37. *Forbes Technology Council. "15 Unexpected Consequences of the GDPR". Forbes. Agosto de 2018. <https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/#42d3f64094ad>*
38. *Freude, Alvar. Freude, Trixy. "Echoes of History: Understanding German Data Protection". Bertelsmann Foundation. Octubre de 2016. <https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/>*

39. *Fridman, Lex. Brown, Daniel. Glazer, Michael. Angell, William. Dodd, Spencer. Jenik, Benedikt. Terwilliger, Jack. Patsekin, Aleksander. Kindelsberger, Julia. Ding, Li. Seaman, Sean. Mehler, Alhea. Sipperley, Andrew. Pettinato, Anthony. Seppelt, Bobbie. Angell, Linda. Mehler, Bruce. Reimer, Bryan. "MIT Autonomous Vehicle Technology Study: Large Scale Deep Learning Based analysis of Driver Behaviour and Interaction with Automation". Massachusetts Institute of Technology. Última actualización abril de 2019. <https://hcai.mit.edu/avt/>*
40. *Gray, Jim. "Evolution of Data Management". Computer, 29 no. 10 (1996): 38-46. <https://pdfs.semanticscholar.org/ba69/4ef52cda8f666d9a0e0aabf2135b7d1b3f7a.pdf>: A59f*
41. *Greengard, Samuel. "Weighting the impact of GDPR". Communications of the ACM. 61 no. 11, (2018), 16-18, <https://cacm.acm.org/magazines/2018/11/232192-weighting-the-impact-of-gdpr/fulltext>*
42. *Grossman, David. "On this Day 25 years ago, the Web Became Public Domain". Popular mechanics. Abril de 2018. <http://radar.oreilly.com/2012/03/data-markets-survey.html>*
43. *Guernion, Yann. "What can automated data analytics do for you?". Ca Technologies. Abril 12 de 2018. <https://www.ca.com/en/blog-automation/what-can-automated-data-analytics-do-for-you.html>*

44. Gulshan, Varun. Peng, Lily. Coram, Marc. "Development and Validation of Deep Learning Algorithm for Detection of Diabetic Retinopathy in Retinal Fundus Photographs". Google. Jama Network. Diciembre de 2016. <https://jamanetwork.com/journals/jama/fullarticle/2588763>
45. "History of the Web". World Wide Web Foundation. No hay fecha. <https://webfoundation.org/about/vision/history-of-the-web/>
46. Hornung, Gerrit. Schnabel, Christoph. "Data Protection in Germany I: The Population Census Decision and the right to information and self-determination". Computer Law and Security Report. Universidad de Kessel. Alemania. 25 no. 1, (229): 1-2, <https://doi.org/10.1016/j.clsr.2008.11.002>
47. Hunton and Williams, "The Proposed EU General Data Protection Regulation A guide for in-house lawyers". Junio de 2015. <https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2015/06/Hunton-Guide-to-the-EU-General-Data-Protection-Regulation.pdf>
48. "Intel Terms of Use". Intel. No hay fecha. <https://www.intel.com/content/www/us/en/legal/terms-of-use.html>
49. International Competition Network. "ICN Merger Guidelines Workbook". Abril de 2006, <http://old.internationalcompetitionnetwork.org/uploads/library/doc321.pdf>

50. Jowitt, Tom. "World's First Business Computer, LEO, Turns 60". *Silicon*. Noviembre de 2011. https://www.silicon.co.uk/workspace/worlds-first-business-computer-leo-turns-60-45618?inf_by=5c1991e3671db8176e8b4577
51. Körber, Torsten. "Data, Platforms and Competition Law". *Comisión Europea*. Diciembre de 2018. http://ec.europa.eu/competition/information/digitisation_2018/media_en.html
52. Lamb, John. "Discriminating Algorithms: 5 times AI showed prejudice". *New Scientist*. Abril de 2018. <https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/>
53. Lancot, Roger. "Accelerating the Future: The Economic Impact of the Emerging Passenger Economy". *Strategy Analytics*. Intel. https://newsroom.intel.com/newsroom/wp-content/uploads/sites/11/2017/05/passenger-economy.pdf?cid=em-elq-26916&utm_source=elq&utm_medium=email&utm_campaign=26916&elq_cid=14942
- 19
54. Ly, Kien Hoa. Ly, Ann-Marie. Andersson, Gerard. "A fully automated conversational agent for promoting mental well-being: A pilot RCT using mixed methods". *Internet Interventions*. 1 no. 10. (2017), 39-46, <https://www.sciencedirect.com/science/article/pii/S221478291730091X/pdf?md5=302ec6d7b88bbb31ec8f94af10f97d58&pid=1-s2.0-S221478291730091X-main.pdf>

55. Mataskis, Luise. "What does a fair algorithm actually look like?". *Wired*. Noviembre de 2018. <https://www.wired.com/story/what-does-a-fair-algorithm-look-like/>
56. Marr, Bernard., "Artificial Intelligence has A Problem With Bias, Here's How to Tackle it". *Forbes*. Enero de 2019. <https://www.forbes.com/sites/bernardmarr/2019/01/29/3-steps-to-tackle-the-problem-of-bias-in-artificial-intelligence/#33ef3877a128>
57. "Millions of small companies aren't GDPR compliant". *GDPR EU*. No hay fecha. <https://gdpr.eu/2019-small-business-survey/>
58. Miranda, Alfonso. Gutiérrez, Juan David. "El Derecho de la Competencia en el Sector Aeronáutico Colombiano". *Revista de derecho de la competencia*. 4 no. 4, (2008): 287-203. <https://centrocedec.files.wordpress.com/2010/06/6-miranda-y-gutierrez.pdf>
59. "Microsoft Services Agreement". *Microsoft*. No hay fecha. <https://www.microsoft.com/en/servicesagreement/>
60. Mostert, Menno. Bredenoord, Annelien. Biesart, Monique. Van Delden, Johannes. "Big Data in medical research and EU data protection law: challenges to the consent or anonymize approach". *European Journal of Human Genetics*, 24 no. 7, (2016), 956-960. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5070890/>
61. Organización para la Cooperación y el Desarrollo Económicos. "Glossary of Industrial Organization Economics and Competition Law". Junio de 2002. <http://www.oecd.org/dataoecd/8/61/2376087.pdf>

62. Organización para la Cooperación y el Desarrollo Económicos. Comité de Competencia. “Barriers to entry”. Mesa redonda sobre política económica. Octubre de 2005. <https://www.oecd.org/daf/competition/abuse/36344429.pdf>
63. Organización para la Cooperación y el Desarrollo Económicos. Comité de Competencia. “Competition and Barriers to Entry”. Enero de 2007. <https://www.oecd.org/competition/mergers/37921908.pdf>
64. Parlamento del Reino Unido. Ley de Protección de Datos. Julio 12 de 1984. http://www.legislation.gov.uk/ukpga/1984/35/pdfs/ukpga_19840035_en.pdf
65. Parlamento Europeo. Comisión Europea. Directiva de Protección de Datos, (95/46/EC). Diciembre 13 de 1995. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES>
66. Parlamento Europeo. Considerando 171 del Reglamento General de Protección de Datos. (EU 2016/679). Abril 27 de 2016. <http://www.privacy-regulation.eu/es/r171.htm>
67. Parlamento Federal Alemán. Ley Federal de Protección de Datos. Enero 27 de 1977. https://www.bgbl.de/xaver/bgbl/media/DD5B0A8907DA04DC249329E46ACA760B/bgb1177i0201_39307.pdf
68. “People: Lothar Determann”. Baker McKenzie. No hay fecha. <https://www.bakermckenzie.com/en/people/d/determann-lothar>.

69. *Primera Convención Europea. Carta de los Derechos Fundamentales de la Unión Europea.* 18 de diciembre de 2000.
http://www.europarl.europa.eu/charter/pdf/text_es.pdf
70. Rossow, Andrew. “The Birth of the GDPR: What Is It And What You Need To Know”. *Forbes*. Mayo de 2018. <https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#729a199055e5>
71. Rouse, Margaret. “Data Marketplace”. *Whatis.com*. Abril de 2015.
<https://whatis.techtarget.com/definition/data-marketplace-data-market>
72. Schüßler, Lennart. Karniyvich, Natallia. “Germany is the First EU Member State to enact new Data Protection Act to align with the GDPR”. *Bird & Bird*. Julio de 2017.
<https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr>
73. Singer, Graham. *History of the Microprocessor and the Personal Computer, Part 2*. *Techspot*. Septiembre de 2014, <https://www.techspot.com/article/884-history-of-the-personal-computer-part-2/>
74. Souris, Elena. Gilman, Hollie. “Data rights are civic rights: a participatory framework for GDPR in the US?”. *Vox*, abril 12 de 2018.
<https://www.vox.com/polyarchy/2018/4/12/17229354/data-rights-civic-rights-gdpr>

75. Stromberg, Joseph. "Herman Hollerith's Tabulating Machine". *Smithsonian*. 9 de diciembre de 2011. <https://www.smithsonianmag.com/smithsonian-institution/herman-holleriths-tabulating-machine-2504989/>
76. Superintendencia de Industria y Comercio. Colombia. Resolución 40912. Junio de 2012.
77. "Tabulating Machine". *History-Computer*. No hay fecha. https://history-computer.com/ModernComputer/Basis/TabulatingMachine_Hollerith.html
78. "Terms for ca.com". *Ca Technologies*. Abril de 2015. <https://www.ca.com/us/legal/terms-for-ca-com.html>
79. "The Colossus Machine". *Stanford Computer Science*. No hay fecha. <https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/colossus.html>
80. "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years". *EU GDPR*. No hay fecha. <https://eugdpr.org/>
81. "The General Data Protection Regulation applies in all Member States from 25 May 2018". *Eur-Lex*. No hay fecha. <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html>

82. *“The Potential Effects of Data Portability Under GDPR”*. Bradley. Noviembre de 2017. <https://www.bradley.com/insights/publications/2017/11/the-potential-effect-of-data-portability-under-gdpr>
83. *“Timeline of Events”*. EU GDPR. No hay fecha. <https://eugdpr.org/the-process/timeline-of-events/>
84. Tribunal Constitucional Alemán. Sentencia del 15 de diciembre de 1983. BVerfGE 65,1 – Censo. Diciembre 15 de 1983. Versión traducida a español. <http://www.servat.unibe.ch/dfr/bv065001.html>
85. Vanberg, Aysem Diker. Bilal Ünver, Mehemet. *“The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?”*. *European Journal of Law and Technology*. 8 no. 1 (2017): 1-22. <http://ejlt.org/article/view/546/727>
86. Walter Suárez. *Entrevista por Santiago Blanco*. Llamada telefónica. Bogotá, Colombia - Alexandria, VA, Estados Unidos. 6 de junio de 2019
87. Wang, Pu. Berzin, Tyler. Romek, Jeremy. Brown, Glissen. Bharadwaj, Shishira. Becq, Aymeric. Xiao, Xun. Liu, Peixi. Li, Liangping. Song, Yan. Zhang, Di. Li, Yi. Xu, Guangre. Tu, Mengtian. Liu, Xiaogang. *“Real-time automatic detection system increases colonoscopic polyp and adenoma detection rates: a prospective randomised controlled study”*. *BMJ*. Febrero de 2019. <https://gut.bmj.com/content/early/2019/02/27/gutjnl-2018-317500>

88. *Watcher, Sandra. Mittelstadt, Bret. Floridi, Luciano. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation". International Data Privacy Law. 7 no. 2, (2017). 76-99. <https://academic.oup.com/idpl/article-pdf/7/2/76/17932196/ipx005.pdf>*
89. *Waxman, Olivia. "The GDPR in Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History". Time Magazine. Mayo 24 de 2018. <http://time.com/5290043/nazi-history-eu-data-privacy-gdpr/>*
90. *"What is automated decision-making including profiling?". Information Commissioner's Office. No hay fecha. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id2>*
91. *Williams, Ann. Brooks, Catherine. Shmargad, Yotam. "How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications". Penn State University Press. 8 no. 1. (2018). 78-115. <https://www.jstor.org/stable/pdf/10.5325/jinfopoli.8.2018.0078.pdf?refreqid=excelsior%3A51bb7a60b2ac8bf8be945d4f0c0d50d4>*

