

Típo de documento: Tesis de maestría

Maestría en Derecho y Economía

Restricciones e ineficiencias económicas creadas en el mercado de datos como consecuencia de la regulación del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos

Autoría: Stello, Luis Francisco

Año de defensa de la tesis: 2022

¿Cómo citar este trabajo?

Stello, L. (2022) "*Restricciones e ineficiencias económicas creadas en el mercado de datos como consecuencia de la regulación del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos*". [Tesis de maestría. Universidad Torcuato Di Tella]. Repositorio Digital Universidad Torcuato Di Tella
<https://repositorio.utdt.edu/handle/20.500.13098/12367>

El presente documento se encuentra alojado en el Repositorio Digital de la Universidad Torcuato Di Tella bajo una licencia Creative Commons Atribución-No Comercial-Compartir Igual 4.0 Argentina (CC BY-NC-SA 4.0 AR)
Dirección: <https://repositorio.utdt.edu>



**UNIVERSIDAD
TORCUATO DI TELLA**

ESCUELA DE DERECHO

MAESTRÍA EN DERECHO Y ECONOMÍA

**RESTRICCIONES E INEFICIENCIAS ECONÓMICAS CREADAS EN EL
MERCADO DE DATOS COMO CONSECUENCIA DE LA REGULACIÓN DEL
DERECHO A NO SER OBJETO DE UNA DECISIÓN BASADA ÚNICAMENTE
EN EL TRATAMIENTO AUTOMATIZADO DE DATOS**

LUIS FRANCISCO STELLO

LEGAJO: 19C1167

TUTOR: FACUNDO MALAUREILLE PELTZER

*A mi compañera de vida, Agustina, por su ayuda y motivación constante durante la
elaboración de esta tesis.*

*A mis padres, por darme la herramienta más valiosa que puede tener una persona para
enfrentar la vida: educación.*

*A mi mejor amigo, Gonzalo, quien me enseñó a vivir la vida con alegría, esfuerzo y
amor.*

TABLA DE CONTENIDO

1. INTRODUCCIÓN	4
1.1. Resumen.....	4
1.2. Objeto y estructura.....	5
1.3. Conclusión	7
2. ANTECEDENTES	8
2.1. Antecedentes históricos de la recolección y tratamiento de datos.....	8
2.2. Antecedentes doctrinarios y jurisprudenciales del derecho a la privacidad y protección de datos personales.....	13
2.3. Antecedentes normativos del RGPD	18
2.4. La Directiva 95/46/CE y el surgimiento del RGPD	21
2.5. Antecedentes y evolución de la regulación en materia de protección de datos personales en la República Argentina. El proyecto para reformar la Ley 25.326	22
3. NOCIONES GENERALES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. ANÁLISIS DEL ARTÍCULO 22	26
3.1. Nociones generales	26
3.2. El artículo 22 del RGPD: Decisiones individuales automatizadas, incluida la elaboración de perfiles	34
4. LA UTILIDAD DE LOS PROCESOS AUTOMATIZADOS DE TOMA DE DECISIONES PARA EL DESARROLLO DE CIERTAS INDUSTRIAS Y CAMPOS DE ESTUDIOS. LAS RESTRICCIONES E INEFICIENCIAS ECONÓMICAS QUE PODRÍA GENERAR EL ART. 22 DEL RGPD	40
4.1. La utilidad e importancia de los procesos automatizados de toma de decisiones. Sus beneficios sobre los consumidores.....	40
4.2. Las restricciones e ineficiencias económicas que podría generar el artículo 22 del RGPD en el mercado de datos	49
5. EXTERNALIDADES NEGATIVAS EN LOS PROCESOS AUTOMATIZADOS DE TOMA DE DECISIONES: LA DISCRIMINACIÓN	60
5.1. La discriminación como fundamento para restringir los procesos automatizados de toma de decisiones	60
5.2. Casos de discriminación de los procesos automatizados de toma de decisiones. 62	62
5.3. Medidas alternativas para erradicar la discriminación y así, aprovechar las ventajas de los procesos automatizados de toma de decisiones.....	65

6. CONCLUSIONES	69
6.1. Las restricciones e ineficiencias económicas creadas en el mercado de datos como consecuencia de la regulación prevista en el artículo 22 del RGPD.....	69
6.2. Conclusión final	71
7. BIBLIOGRAFÍA	73

1. INTRODUCCIÓN

1.1. Resumen

A partir del avance de las nuevas tecnologías y el desarrollo en materia de privacidad, nuevas regulaciones han sido sancionadas por ciertos parlamentos a los fines de proteger los derechos de los consumidores y cubrir lagunas legales. En particular, cabe señalar que algunas normas -como el Reglamento General de Protección de Datos de la Unión Europea (en adelante, el “RGPD”)- en su afán de resguardar derechos individuales podrían generar ineficiencias económicas y desalentar el desarrollo del mercado de datos.

Así, en el presente trabajo analizaré la regulación prevista en el artículo 22 del RGPD y las eventuales consecuencias que la misma podría causar en el mercado de datos, en la libre competencia económica y en los derechos de los consumidores; demostrando en paralelo, cómo dicha norma crea restricciones e ineficiencias económicas que afectan directamente al mercado de datos e indirectamente a los consumidores.

Palabras clave: RGPD, datos personales, mercado de datos, tratamiento automatizado de datos, efectos jurídicos, profiling.

Abstract

Certain parliaments have released a wide range of laws in order to protect consumers’ rights throughout recent years, since new technologies and data privacy have increased the scope of its development. Thus, I will indicate that some norms, such as The General Data Protection Regulation, by intending to protect consumers’ rights could make economic inefficiencies and deter development of the data privacy market and economic competition.

In this paper, I will analyse the General Data Protection Regulation (specifically, chapter 22) and its consequences on data privacy market and consumers’ rights. To

demonstrate how this regulation can cause economic inefficiencies affecting data privacy market and consumers.

Key words: GDPR, data privacy, data privacy market, automated decision making, legal effects, profiling.

1.2. Objeto y estructura

Conforme con lo adelantado en el resumen precedente, el propósito de este trabajo consiste en demostrar que la regulación prevista en el artículo 22 del RGPD -en su intento de proteger los derechos de los consumidores- podría generar restricciones e ineficiencias en el mercado de datos y la libre competencia económica; y que a su vez, podría causar un daño indirecto en los consumidores, dado el incremento de precios y el desincentivo a la innovación y desarrollo tecnológico que dichas ineficiencias podrían causar.

En el **capítulo 2** comenzaré relatando los antecedentes históricos, doctrinarios, jurisprudenciales y normativos que dieron origen al tratamiento automatizado de datos personales y al RGPD, para entender el contexto en virtud del cual se reguló el derecho “...a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos...”¹. Para ello, se expondrá sobre la evolución de la recolección y tratamiento de datos.

Una vez sentados estos antecedentes, me referiré a la norma antecesora del RGPD; esta es, la Directiva de Protección de Datos (1995); y finalmente, señalaré -de forma breve- el surgimiento del RGPD, su aprobación por los Estados miembros y su entrada en vigor el 25 de mayo de 2018. Ello, a los efectos de introducir dicha norma para analizarla con mayor detalle en el capítulo siguiente.

En paralelo, y ya expuestos los antecedentes del RGPD, mencionaré los antecedentes argentinos en materia de regulación de datos personales y cuál es la situación actual del país frente al surgimiento del reglamento europeo.

¹ Artículo 22, apartado 1 del RGPD.

En el **capítulo 3** se expondrá de manera preliminar sobre algunas nociones generales del RGPD. Al respecto, dicho reglamento ha sido catalogado como una regulación muy estricta en el campo de la protección de datos². En este sentido, y si bien algunas compañías como Microsoft han manifestado que el RGPD es una regulación estricta pero innovadora que permitirá el desarrollo en materia de privacidad³, cabe señalar que dicha normativa también podría provocar consecuencias negativas para las compañías que obtienen, almacenan y procesan datos. Respecto a este punto, se darán ciertos ejemplos para ilustrar los efectos adversos que podría causar la aplicación del art. 22 de este reglamento, como ser –por ejemplo- el incremento de costos para que pequeñas y medianas empresas puedan operar en el mercado de datos, de acuerdo a las exigencias requeridas por dicha norma.

También se explicará la aplicación territorial del RGPD, ya que el mismo aplica al tratamiento de datos personales de ciudadanos que se encuentran en la Unión Europea, por parte de empresas que pueden -o no- estar situadas en el territorio de un país de dicha comunidad⁴.

Sentado lo anterior, se pasará a realizar un análisis pormenorizado del art. 22 del RGPD. A tal fin, se explicará los alcances e implicancias de dicho artículo, qué son las decisiones automatizadas y el profiling, así como qué se entiende por “efectos jurídicos”. A la vez, se detallarán las excepciones contenidas en dicho artículo y se expondrán las dificultades interpretativas del mismo.

Además, desarrollaré sobre qué categorías especiales de datos personales (contenidas en el art. 9, apartado 1 del RGPD) no pueden basarse las decisiones/excepciones enunciadas en el artículo 22.

En el **capítulo 4** me expediré sobre la utilidad y usos que los procesos automatizados de toma de decisiones pueden tener en ciertas industrias como la financiera, automotriz, construcción y/o campos de estudio como la medicina o recursos

² Matt Burges, “*What is GDPR? The summary guide to GDPR compliance in the UK*”, recuperado el 14 de diciembre de 2020 de www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

³ Julie Brill, “*GDPR’s first anniversary: A year of progress in privacy protection*”. 2019.

⁴ Artículo 3, apartado 3 del RGPD.

humanos. Así, explicaré por qué el desarrollo de esas industrias y/o disciplinas requieren necesariamente de procesos automatizados de toma de decisiones; y en paralelo, mencionaré algunas ventajas que dichos sistemas representan en términos de eficiencia y reducción de costos.

Explicado lo anterior, procederé a desarrollar la idea de cómo la regulación prevista en el artículo 22 del RGPD podría generar restricciones e ineficiencias económicas en el mercado de datos y en la libre competencia económica. En particular, señalaré que dicha regulación podría (i) crear una barrera legal a la entrada; (ii) ser un desincentivo para la innovación tecnológica; y (iii) causar una mayor concentración en el mercado de datos.

En el **capítulo 5** se explicará que ciertas externalidades negativas derivadas de los procesos automatizados de toma de decisiones (la discriminación) tienen su origen en factores externos -como la información que es incorporada y utilizada en dichos procesos-, no siendo la limitación de estos procesos la mejor solución al problema.

Aquí se ilustrarán ciertos casos prácticos en los cuales la discriminación realizada por los procesos automatizados de toma de decisiones proviene del input incorporado por los programadores y no del algoritmo y/o procesador en sí mismo. Precisamente, uno de los argumentos utilizados para defender la regulación prevista en el artículo 22 es la discriminación de la información efectuada por dichos procesos automatizados. Sin embargo, ello no justifica la restricción establecida en el RGPD, dado que podrían adoptarse medidas alternativas para mejorar esos efectos adversos. Todo el análisis de ello se realizará en el capítulo mencionado a los fines de exponer en la sección siguiente sobre una eventual solución/alternativa a los efectos adversos.

1.3. Conclusión

Finalmente, en el **capítulo 6** desarrollaré las conclusiones de los puntos analizados en el presente trabajo y de la hipótesis de investigación planteada.

2. ANTECEDENTES

En este capítulo, se relatarán los antecedentes históricos, normativos, doctrinarios y jurisprudenciales que dieron origen y/o contribuyeron al dictado del RGPD; ello, a fin de que el lector tome conocimiento de los hechos, causas y contexto en virtud de los cuales se reguló el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos.

A su vez, señalaré los antecedentes argentinos en materia de regulación de datos personales y me expediré sobre la situación actual de nuestro país frente al surgimiento de las nuevas regulaciones en esta materia; como es, el RGPD.

2.1. Antecedentes históricos de la recolección y tratamiento de datos

El primer antecedente de recolección de datos podría adjudicársele a la cultura sumeria (que para situar al lector se ubicó en Medio Oriente entre los años 3.500 - 3.000 A.C.), que registraba en tablas de arcilla los datos relativos a los bienes que poseían los reyes, a la contabilidad, a las batallas ocurridas, a la literatura de la época, entre otros; ello, mediante el sistema de escritura cuniforme⁵.

Luego, para el año 2.400 A.C., comenzaron a fundarse las primeras bibliotecas en Babilonia, en las cuales se almacenó el conocimiento y datos correspondientes a dicha época. Así, ya en el año 200 D.C. se dio la invención del mecanismo de



anticitera en Grecia, mecanismo que para muchos es considerado el primer ordenador mecánico de la historia⁶. Básicamente, el mecanismo de anticitera fue una computadora

⁵ Samuel Noah Kramer, *“La historia empieza en Sumer”*, Ediciones Orbis SA, 1985, pág. 17-21.

⁶ José Antonio Castillo Romero, *“Big Data. IFCT128PO”*, Ed. Ic, 2018, pág. 7.

análoga utilizada por los griegos para predecir las posiciones del sol, la luna y los planetas, así como los eclipses lunares y solares.

Una de las invenciones que aceleró y colaboró con la recolección de datos fue la imprenta (1453). Antes de la creación de Johannes Gutenberg, las únicas fuentes de peso en la sociedad eran los manuscritos emitidos por monjes -en los cuales se hallaban los datos de relevancia social-, cuya redacción era solicitada por el clero de la iglesia católica y/o los reyes⁷. Así, la invención de la imprenta masificó la recolección y difusión de datos de todo tipo, logrando que la registración de datos y análisis de los mismos pudiera ser realizado por cualquier individuo de la sociedad y no solo por la burguesía.

A finales del siglo XIX (1890) y con causa en el censo nacional llevado adelante por el Gobierno de los Estados Unidos, un nuevo invento permitió desarrollar aún más la recolección y tratamiento de datos: la maquina tabuladora de Herman Hollerith. Esta máquina procesaba información -de manera organizada y rápida- codificada en tarjetas perforadas. Cada agujero de la tarjeta representaba cierta información recolectada sobre las personas censadas, permitiendo que la información recogida en el censo pudiera ser tratada en no más de tres años⁸. En este punto, cabe destacar el avance que significó el invento del ingeniero germano-estadounidense, dado que con anterioridad a la creación de la maquina tabuladora, el Gobierno de los Estados Unidos tardaba diez años en procesar y analizar la información proveniente de censos nacionales.

Tan exitoso fue el avance en el procesamiento de datos y el ahorro de costos (se estima que el Gobierno estadounidense se ahorró cinco millones de dólares gracias al uso de la maquina tabuladora⁹), que luego de ser utilizada en el censo de Estados Unidos, dicha maquina comenzó a emplearse en el censo de países como Rusia, Austria, Canadá, Francia, Noruega, Puerto Rico, Cuba, y Filipinas¹⁰.

⁷ Inés Lujan, “*La imprenta y su impacto en la historia*”, Universidad de Valencia, recuperado el 1 de abril de 2021 de <https://www.uv.es/uvweb/master-historia-formacion-mundo-occidental/es/blog/invencion-imprenta-impacto-historia-1285960141137/GasetaRecerca.html?id=1285961209839>.

⁸ Frank da Cruz, “*Herman Hollerith*”, Columbia University, 2021, recuperado el 1 de abril de 2021 de <http://www.columbia.edu/cu/computinghistory/hollerith.html>.

⁹ *Ibíd.*

¹⁰ *Ibíd.*

En este contexto, Herman Hollerith fundó su propia compañía (Tabulating Machine Company) que luego se fusionaría con otras empresas para pasar a conformar la Internacional Business Machines, más conocida como “IBM”¹¹.

Con posterioridad a ello, en el año 1928, se produjo un nuevo avance en la recolección y tratamiento de datos. Fritz Pfleumer patentó el sistema magnético de almacenamiento de datos, por el cual se almacenaba sonido en una cinta magnética¹². Así, en 1932 la empresa German General Electric (AEG) compró los derechos de patente de Pfleumer y comenzó a desarrollar -basándose en la idea del ingeniero austriaco- una máquina que luego fue conocida como el Magnetophon; que fue, básicamente, una grabadora de sonido en una escala mayor a la diseñada por Pfleumer. Al respecto, cabe señalar que la primera grabación hecha a través del Magnetophon fue realizada en la ciudad alemana de Ludwigshafen am Rhein el 19 de noviembre de 1936¹³. Años más tarde (1950), IBM comenzaría a emplear una tecnología muy similar a la utilizada en el Magnetophon para almacenar datos.

Así, vemos cómo la forma en que se recolectaban los datos fue evolucionando con el paso del tiempo.

Tal vez, el hecho que cambió para siempre la forma de almacenar datos y analizar los mismos fue la creación del computador, el que fue creado por Konrad Zuse (1938) en el departamento de sus padres en Berlín durante la Segunda Guerra Mundial¹⁴.



Al respecto, cabe señalar que durante la Segunda Guerra Mundial los países aliados crearon dos ordenadores que contribuyeron al desarrollo de la recolección y tratamiento de datos; estos son, el Colossus Mark I en Inglaterra y el Electronic Numerical

¹¹ José Antonio Castillo Romero, “*Big Data. IFCT128PO*”, Ed. Ic, 2018, pág. 7.

¹² Ibid.

¹³ Ranjit Kaur, Parveen Kumar, Raminder Pal Singh, “*A Journey of Digital Storage from Punch Cards to Cloud*”, IOSR Journal of Engineering (IOSRJEN), 2014, pág. 37.

¹⁴ Konrad Zuse, “*The computer – My life*”, Ed. Springer Verlag, 1984, 1986, 1990, 1993, pág. 32-35.

Integrator And Computer (ENIAC) en Estados Unidos. Así, el Colossus Mark I fue creado para descifrar los mensajes alemanes encriptados y emitidos por la máquina de cifrado Lorenz SZ-40/42¹⁵, mientras que el ENIAC no pudo ser utilizado de manera plena en la guerra, ya que la misma finalizó antes de su lanzamiento efectivo -fue presentado el 15/2/1946¹⁶-, por lo que dicha maquina terminó siendo empleada para resolver problemas relacionados con el desarrollo de la bomba de hidrógeno¹⁷.

En este sentido, vemos que durante este período de la historia humana, la recolección de datos no estaba vinculada con datos personales, sino con mensajes y estrategias de uso militar. Sin embargo, sin el avance realizado con estos ordenadores, no hubiera sido posible el desarrollo de computadoras de primera generación años más tarde.

Por ejemplo, gracias a los avances generados por el ENIAC, Charney y Eliassen diseñaron el primer modelo de predicción meteorológica (1949)¹⁸. Este sistema utilizaba un modelo físico-matemático que analizaba datos atmosféricos y geográficos para predecir el clima y gracias a su empleo se logró reducir el tiempo y costos de realización de dicha tarea. Este modelo permitió que entre las décadas del 50' y 70' se haya agilizado la comercialización de sistemas de tratamiento de datos¹⁹.

Luego, entre los años 1970 y 1980, la comercialización masiva del computador personal y el desarrollo del microprocesador causó que la población en general pudiera acceder a estos sistemas de recolección y tratamiento de datos, acceso que hasta ese entonces solo habían tenido las entidades gubernamentales y las grandes compañías²⁰.

¹⁵ Crypto Museum, “*Colossus of the Digital Computer*”, recuperado el día 2 de abril de 2021 de <https://www.cryptomuseum.com/crypto/colossus/index.htm#:~:text=Birth%20of%20the%20digital%20computer&text=It%20was%20used%20to%20break,before%20the%20American%20ENIAC%20computer>.

¹⁶ Institució Alfons el Magnànim-Centre Valencià d'Estudis i d'Investigació “*El primer ordenador del mundo cumple años*”, recuperado el día 2 de abril de 2021 de <http://www.conec.es/historia/%E2%80%A8el-primer-ordinador-del-mon-compleix-anys/>.

¹⁷ Engeniering and Technology, “*ENIAC*” recuperado el día 2 de abril de 2021 de <https://ethw.org/ENIAC>.

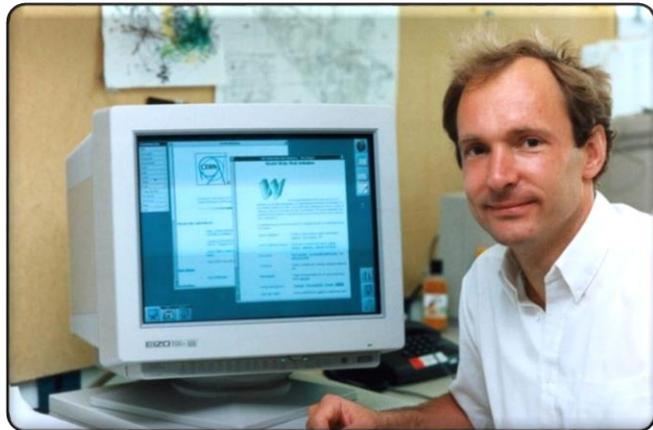
¹⁸ J. G. Charney – A. Eliassen, “*A Numerical Method for Predicting the Perturbations of the Middle Latitude Westerlies*”, *Tellus*, 1:2, 38-54, DOI: 10.3402/tellusa.v1i2.8500.

¹⁹ Peter Lynch, “*The origins of computer weather prediction and climate modeling*”, *Journal of Computational Physics*, 2008, pág. 3431-3444.

²⁰ Graham Singer, “*History of the Microprocessor and the Personal Computer, Part 2*”, obtenido el 2 de abril de 2021 de <https://www.techspot.com/article/884-history-of-the-personal-computer-part-2/>.

Por otra parte, sin duda otra de las grandes invenciones que cambió la manera de recolectar datos y tratar los mismos fue la World Wide Web (en adelante, la “web”) en 1990. Al respecto, la web fue una creación de Tim Berners-Lee, quien al trabajar en la Organización Europea para la Investigación Nuclear (CERN) se dio cuenta que resultaba difícil compartir información entre las computadoras de dicho centro de investigación. Berners-Lee encontró la manera de resolver este problema: utilizaría una nueva tecnología emergente conocida como el hipertexto²¹. Pero no le fue fácil.

En marzo de 1989, Tim mostró a su jefe (Mike Sendall) un documento llamado “Dirección de información: una propuesta” en el cual expresaba su visión y propuesta para conectar a millones de computadoras en el mundo. Lamentablemente, su propuesta no



fue aceptada inicialmente. Sin perjuicio de ello, Sendall le dio tiempo a Berners-Lee para que trabajara en su idea y para octubre de 1990, éste último creó el primer navegador web (es un software que permitía el acceso a la web interpretando la información de distintos tipos de archivos y sitios web para que estos pudieran ser vistos) y para fines de ese año, la primera página web estuvo cargada y disponible en la internet²².

Pero más allá de la importancia del invento de Berners-Lee, lo que realmente permitió la conexión e interacción entre los ordenadores de todo el mundo fue la declaración de dominio público de la web.²³ En este punto, cabe señalar que el acceso público a internet y la libre disponibilidad de información constituirían el primer paso para el surgimiento del mercado de datos.

²¹ World Wide Web Foundation, “History of the Web”, no tiene fecha, <https://webfoundation.org/about/vision/history-of-the-web/>.

²² *Ibid.*

²³ Silvia Lago Martínez, “Ciberespacio y resistencias. Exploración en la cultura digital”, Hekht libros, 2012, pág. 57.

Ahora bien, inicialmente la web era simplemente una colección de textos estáticos que podían consultarse y/o descargarse. Así, el siguiente paso en su evolución fue la inclusión de un nuevo método -conocido como Common Gateway Interface (CGI)- para confeccionar páginas dinámicas, que trajo como consecuencia el surgimiento de las aplicaciones web (1994)²⁴. En términos simples, una aplicación web es un programa o conjunto de programas que ayuda al usuario de un ordenador a realizar una tarea determinada. Por ejemplo, el buscador de Google es una aplicación web que permite al usuario realizar una tarea determinada: la búsqueda de información y/o contenido en otras páginas de internet.

En este sentido, cabe señalar que la utilización de las aplicaciones web está vinculada de manera directa con la recolección y tratamiento de datos personales, dado que al interactuar el usuario con las mismas, todo lo que hace en la aplicación se procesa y almacena en el interior de una base de datos²⁵; y dicha información luego es tratada para tomar una decisión con relación a dicho usuario -lo que más adelante desarrollaremos como el profiling-.

Sentados los antecedentes históricos, a continuación, pasaré a desarrollar ciertos antecedentes doctrinarios y jurisprudenciales que fueron modelando la noción del derecho a la privacidad -y la necesidad de su protección- y que dieron lugar a su posterior reconocimiento y regulación normativa en el RGPD.

2.2. Antecedentes doctrinarios y jurisprudenciales del derecho a la privacidad y protección de datos personales

Como suele ocurrir con gran parte de los derechos y obligaciones relativos al ser humano y a su comportamiento social, el derecho a la privacidad fue reconocido primeramente por construcciones doctrinarias y jurisprudenciales; y luego, mediante la sanción de normas legales.

²⁴ Sergio Luján Mora, “Programación de aplicaciones web: historia, principios básicos y clientes web”, Ed. Club Universitario, 2002, pág. 27-28.

²⁵ I. Kuster – A. Hernandez, “De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención de uso de las redes sociales en la web semántica”, *Universia Business Review*, 2013, pág. 111-119.

En este sentido y de manera preliminar, cabe señalar que el nacimiento del derecho a la privacidad (*privacy*²⁶) y el reconocimiento de este derecho como tal, surge en Estados Unidos a finales del siglo XIX (1890)²⁷. Si bien con anterioridad a dicho año, ya existían algunas aproximaciones doctrinales del derecho a la privacidad realizadas por el juez Thomas M. Cooley²⁸, lo cierto es que el punto de partida de este derecho fue el artículo “*The right to privacy*” publicado por Samuel Warren y Louis Brandeis en la Harvard Law Review en diciembre de 1890²⁹.

Este artículo fue escrito a raíz de ciertas publicaciones realizadas por los medios gráficos locales de Boston -donde residía Warren- con respecto a la vida privada de Warren y su familia.

Al respecto, con motivo de las publicaciones realizadas sobre la boda de una de las hijas de Warren -ceremonia que había sido realizada en su casa-, este abogado se sintió agraviado y decidió acudir a Louis Brandeis para que lo ayudara a determinar si el ordenamiento jurídico de esa época protegía el derecho a la privacidad³⁰. Como consecuencia de ello, ambas personas publicaron un artículo en el cual se establecieron ciertos límites jurídicos a la invasión de la prensa en el ámbito privado de las personas.

En particular, en este artículo se entendió “...*el derecho a la privacidad como el rechazo de toda intromisión no consentida en la vida privada de una persona, sobre todo, de los medios de comunicación, haciendo prevalecer las ideas de aislamiento y autonomía especialmente en aspectos de la vida doméstica y las relaciones sexuales.*”³¹

²⁶ Aquí, cabe aclarar que una traducción aproximada al castellano de *privacy right* sería derecho a la intimidad, pero como el derecho a la intimidad engloba otros principios y protege otro bien jurídico, seguiré expresando derecho a la privacidad como traducción de *privacy right*.

²⁷ Víctor, Cazorro Barahona, “*Antecedentes y fundamentos del derecho a la protección de datos*”, Ed. Bosh, 2020, pág. 19.

²⁸ Quien en su obra “*The Elements of Torts*” (1873), define el ahora derecho a la privacidad como “*The right to be let alone*”, es decir, el derecho a ser dejado solo o de no ser perturbado o molestado por injerencias externas no deseadas.

²⁹ S. Warren – L. Brandeis, “*The right to privacy*”, 4 Harvard Law Review, 193, December 15, 1890.

³⁰ Ernesto Clímaco Valiente, “*Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento*”, Universidad III Carlos de Madrid, 2012, pág. 16-17.

³¹ *Ibíd.*

Dicha obra pasaría a convertirse en un aporte fundamental en la literatura jurídica del derecho a la privacidad, y en particular, en la protección de datos personales.

Así, el derecho a la privacidad -entendido en un primer momento como el derecho a ser dejado en soledad- comenzó a ser considerado y definido como tal por la jurisprudencia de Estados Unidos en casos como *“Bretns vs. Morgan”* (1927)³². En este caso, el Sr. Bretns tenía un negocio en su garaje y el Sr. Morgan mantenía una deuda con él de \$ 49,67 dólares; dado ello, Bretns en reiteradas ocasiones había advertido a Morgan que si no saldaba su deuda, exhibiría un cartel en el cual daría a conocer dicha situación públicamente. Morgan le prometió muchas veces que saldaría su deuda, pero nunca lo hizo.

Entonces, Bretns hizo un cartel y lo exhibió en la ventana de su garaje -que daba a la calle principal del pueblo-. En el cartel, Bretns expuso que *“El Dr. W.R Morgan debe en su cuenta la suma de \$ 49,67. Si las promesas pagaran las cuentas, su deuda habría sido saldada mucho tiempo atrás. Este aviso seguirá publicado hasta tanto la deuda del Sr. Morgan permanezca impaga”* (traducción propia)³³.

Como consecuencia de ello, Morgan inició una demanda contra Bretns alegando que el cartel exhibido en la ventana de su garaje le había causado humillación y ciertos daños morales, y que el mismo solo tenía como propósito generar una mala reputación de Morgan en la sociedad. En este contexto, y habiendo Morgan apelado la resolución de primera instancia, la Cámara de Apelaciones de Kentucky entendió el derecho a la privacidad como *“...el derecho que tiene cada persona de no ser objeto de una publicidad ilegal; el derecho de vivir sin interferencias ilegales del público en lo concerniente a asuntos en los cuales ese público no tiene un interés legítimo...”*³⁴ (traducción propia). Finalmente, la Cámara ordenó a Bretns indemnizar a Morgan por haber realizado aquella publicación que se inmiscuía en la esfera privada del actor y divulgaba datos personales del mismo.

³² Court of Appeals of Kentucky, *“Bretns vs. Morgan”*, 15/11/1927, obtenido el 17 de abril de 2021 de <https://www.casemine.com/judgement/us/5914a723add7b049346e74a1>.

³³ *Ibíd.*

³⁴ *Ibíd.*

En esta línea, muchos fueron los casos en los cuales los tribunales estadounidenses delimitaron el alcance y contenido del derecho a la privacidad. Por ejemplo, en “*Olmstead vs. United States*” (1928), el mismo Louis Brandeis -que para ese entonces era ministro de la Corte Suprema de Estados Unidos- sostuvo en su voto disidente que la cuarta enmienda no protegía el derecho de propiedad, sino el derecho a ser dejado en soledad (the right to be let alone), ampliando el ámbito de protección garantizada literalmente por ésta³⁵.

Asimismo, en el caso “*Griswold vs Connecticut*” (1965), la Corte Suprema de los Estados Unidos definió el derecho a la intimidad/privacidad como un derecho autónomo y específico, como una verdadera emancipación de cualquier otro derecho y como un parámetro único para la toma de decisiones íntimas³⁶.

En virtud de dichos antecedentes, vemos cómo antes de la sanción de cualquier norma que regulara el derecho a la privacidad y los datos personales, ya la jurisprudencia había reconocido tal derecho y su necesidad de protección.

Así las cosas, cabe remarcar que el contenido y alcance del derecho a la privacidad fue estudiado y desarrollado en un primer momento por ciertos autores y jueces estadounidenses; tales como, Thomas Cooley, Samuel Warren, Louis Brandeis, William Prosser³⁷, Edward Bloustein³⁸, entre otros. Pero luego, el avance y lineamiento de dicho derecho fue desarrollado también por la doctrina y jurisprudencia continental europea.

El primer acercamiento europeo al derecho a la privacidad -y más precisamente a su regulación- fue el realizado por Lord Mancroft en Inglaterra en el año 1961, quien preocupado por la intromisión de los medios de comunicación en la esfera privada de las personas, presentó un proyecto de ley ante la Cámara de los Lores que pretendía regular

³⁵ Supreme Court of The Unites States, “*Olmstead et al. v. United States*”, 4/6/1965, obtenido el día 18 de abril de 2021 de <https://www.law.cornell.edu/supremecourt/text/277/438>.

³⁶ Supreme Court of The Unites States, “*Estelle T. Griswold et al. Appellants, v. State of Connecticut*”, 7/6/1965, obtenido el día 18 de abril de 2021 de <https://www.law.cornell.edu/supremecourt/text/381/479>.

³⁷ William Prosser, “*Privacy*”, California Law Review v. 98, 1960 (divide la protección de la privacidad en cuatro categorías dentro del derecho de daños).

³⁸ Edward Bloustein, “*Privacy, Tort Law, and Constitution: Is Warren and Brandeis’ tort petty and unconstitutional as well?*”, Texas Law Review, v. 46, 1968 (plantea una crítica al concepto de derecho a la privacidad realizado por Warren y Brandeis a la luz de ciertos fallos judiciales).

el derecho a la privacidad de las personas. El proyecto y su contenido establecían, principalmente, la idea de un derecho general a la privacidad que debía ser respetado por los diarios, el cine, la radio y la televisión, quienes en principio no tenían responsabilidad por dar publicidad de los asuntos de una persona cuando ésta no daba su consentimiento.

Ahora bien, sin perjuicio de que dicho proyecto no terminó convirtiéndose en ley, éste fue el primer intento realizado en Europa para proteger los datos personales de las personas.

Por su parte, otro antecedente importante que tuvo influencia en la regulación de la protección de datos europeos fue el fallo del Tribunal Constitucional Federal Alemán (15 de diciembre de 1983)³⁹ respecto de la inconstitucionalidad de la Ley del Censo de Población de 1983.

Al respecto, el 5 de marzo de 1983 las abogadas Wild y Stadler-Euler promovieron una acción de amparo contra el Estado alemán por entender que la Ley del Censo de Población lesionaba los derechos y garantías fundamentales previstos en los artículos 1, 2, 5 y 19 de la Ley Fundamental de la República Federal Alemana. Estos eran, (i) el derecho al libre desenvolvimiento de la personalidad, en relación con el derecho a la dignidad humana; (ii) el derecho a la libre expresión de la opinión y (iii) el derecho a la garantía procesal⁴⁰.

Así, el Tribunal Constitucional Federal Alemán resolvió que la Ley del Censo era parcialmente inconstitucional dado que contrariaba los artículos 1 y 2 de la Constitución alemana; y en paralelo, reconoció la existencia del “*derecho a la autodeterminación informativa*”.

Para el tribunal, **el reconocimiento de este derecho implicaba la garantía de que todo individuo pudiera decidir libremente si la información relativa a su persona podía -o no- ser revelada y difundida. Antecedente directo del derecho a no**

³⁹ Tribunal Constitucional Alemán, 15/12/1983, BVerfGE 65,1 obtenido el día 18 de abril de 2021 de <https://revistasonline.inap.es/index.php/DA/article/view/4687/474>.

⁴⁰ *Ibíd.*

ser objeto de una decisión basada únicamente en el tratamiento de datos automatizado.

Y como consecuencia de dicho fallo, el censo poblacional planeado para el año 1983 fue suspendido hasta 1987; y a su vez, la Ley de Protección de Datos alemana de 1977 debió ser repensada y modificada por la Ley Federal de Protección de Datos (20 de diciembre de 1990)⁴¹.

En esta línea, cabe destacar que el derecho y la jurisprudencia alemana tuvieron una particular influencia en la legislación europea respecto a la protección de datos personales. Influencia que luego se terminaría plasmando en el RGPD.

Sentado lo expuesto, vemos como el derecho a la privacidad y la protección de la información personal fue una cuestión que, en primera medida, fue reconocida por la doctrina y jurisprudencia; y luego, a partir de su expansión y reconocimiento, fue regulada normativamente por los distintos países del mundo. Regulación legal de la que terminó surgiendo el RGPD.

Es por ello que a continuación, pasaré a desarrollar los antecedentes normativos que regularon el derecho a la privacidad y la protección de los datos personales, que constituyeron los precedentes de la legislación contemporánea y que tuvieron influencia en el dictado de la nueva normativa europea en materia de protección de datos personales: el RGPD.

2.3. Antecedentes normativos del RGPD

El primer precedente normativo relevante en materia de protección de datos personales fue la Declaración Universal de los Derechos Humanos (1948), que en su artículo 12 enuncia que *“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.*

⁴¹ 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).

Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”⁴².

En esta línea, la Convención en Europa de Derechos Humanos (1950) en su artículo 8 resguardó el derecho a la vida privada y familiar estableciendo que “*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y correspondencia.*”⁴³.

Con posterioridad al dictado de dichas normas fundamentales en materia de derechos humanos, más precisamente luego de la década del 60’, se comenzó a expandir en Europa una corriente tendiente a reconocer normativamente el derecho a la privacidad -y en particular, en cuanto a la recolección y tratamiento de datos-; en este sentido, ciertos países de Europa fueron sancionando leyes que protegían los datos personales de sus ciudadanos.

Al respecto, **en el año 1970 se sancionó la que sería conocida como la primera ley de protección de datos del mundo; esta fue, la Ley de Protección Datos del Estado de Hesse en Alemania**⁴⁴. Fue una norma histórica en esta materia, relativa al control de los actos y procedimientos de la administración pública del *Land*⁴⁵. A pesar de sus limitaciones en punto a su aplicación territorial y a su contenido, esta ley causó un gran interés en el mundo del derecho no solo dentro de Alemania, sino también en los demás países de la región.

Esta ley contenía aspectos muy particulares que regulaban, por ejemplo, la utilización de los centros de información electrónica de datos administrados por las autoridades públicas; y a su vez, se creaba también un órgano de contralor (el

⁴² Organización de las Naciones Unidas, “*art. 12 de la Declaración Universal de los Derechos Humanos*”, 10/12/1948, obtenido el 20 de abril de 2021 de <https://www.un.org/es/universal-declaration-human-rights/>.

⁴³ Consejo de Europa, “*art. 8 de la Convención Europea de Derechos Humanos*” 3/9/1950, obtenido el 20 de abril de 2021 de <https://www.derechoshumanos.net/Convenio-Europeo-de-Derechos-Humanos-CEDH/#a8>.

⁴⁴ Parlamento Federal Alemán, “*Ley Federal de Protección de Datos*”, 27/1/1977, obtenido el 21 abril de 2021 de https://www.bgbl.de/xaver/bgbl/media/DD5B0A8907DA04DC249329E46ACA760B/bgbl177i0201_3_9307.pdf.

⁴⁵ Land era la denominación para los estados federados de la República Federal Alemana.

“Datenschutzbeauftragter”) con una función específica relacionada con la gestión de los ordenadores públicos. Tal fue la repercusión de dicha norma, que el Parlamento de la República Federal Alemana sancionó la Ley Federal de Protección de Datos en el año 1977. Básicamente, esta ley federal regulaba la protección de datos personales a nivel nacional, no como aquella norma sancionada en 1970 que regía solo para el Estado de Hesse.

Otros países de Europa también avanzaron en la regulación y protección de datos personales (en la década del 70'). En este sentido, Suecia sancionó su Ley de Protección de Datos (“Datalegen”) en 1973⁴⁶; lo propio hizo Francia regulando la protección de datos personales mediante la “Loi 78-17” en 1976⁴⁷; como así también Dinamarca, que en el año 1978 aprobó en un mismo día (el 8 de junio de 1978) dos leyes de protección de datos -complementarias entre sí- que se ocupaban, respectivamente, del tratamiento de datos del sector privado (Ley 293) y público (Ley 294)⁴⁸.

Siguiendo con esta evolución normativa, cabe destacar que el 28 de enero de 1983, el Consejo Europeo dictó otro precedente normativo muy importante para la protección de datos personales; este fue, el “Convenio para la Protección de las Personas con respeto al Tratamiento Automatizado de Datos de Carácter Personal” (en adelante, el “Convenio 108”).

En los considerandos de dicho convenio, se estableció expresamente que era “...deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.” Así, cabe señalar que con dicha norma se empezó a reconocer el avance e incremento del tráfico de datos personales entre

⁴⁶ Asamblea Legislativa del Reino de Suecia, “Datalegen”, 11/5/1978, obtenido el 21 de abril de 2021 de <http://rkrattsbaser.gov.se/sfst?bet=1973:289>.

⁴⁷ Asamblea Nacional de Francia, “Ley 78-17 sobre datos, archivos y libertades”, 6/1/1978, obtenido el 21 de abril de 2021 de <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460>.

⁴⁸ Dinamarca, *Lov nr. 293 om private registre m.v. af 8. juni 1978* [Ley número 293 sobre los ficheros privados, de 8 de junio de 1978]. *Lovtidende*, A, 1978, 833; Dinamarca. *Lov nr. 294 om offentlige myndigheders registre af 8. juni 1978* [Ley número 294 sobre los ficheros públicos, de 8 de junio de 1978].

los países de Europa; y a su vez, se comenzó a hacer foco en el tratamiento automatizado de los mismos.

Concretamente, el objeto de este convenio era garantizar el “...*derecho a la vida, con respecto al tratamiento automatizado de los datos de carácter personal correspondiente a dicha persona...*”⁴⁹ entendiendo al tratamiento automatizado de datos como “...*las operaciones que a continuación de indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.*”⁵⁰. De esta norma, se tomarían muchos conceptos y principios jurídicos para lo que luego se regularía en el art. 22 del RGPD.

2.4. La Directiva 95/46/CE y el surgimiento del RGPD

Ahora bien, pese al dictado del Convenio 108, en Europa persistía la necesidad de brindar una mayor protección de las personas frente al tratamiento automatizado de sus datos; y de asegurar un nivel de protección adecuado entre los diversos Estados frente al incremento de flujo transfronterizo de datos personales. Entonces, el Parlamento y el Consejo de la Unión Europea considerando las deficiencias que mostraba el Convenio 108 para regular dichas cuestiones, dictó una directiva que sería el antecedente directo del RGPD: La Directiva de Protección de Datos (Directiva 95/46/CE) del 24 de octubre de 1995⁵¹.

Mediante esta directiva se ampliaron las condiciones generales y previsiones que el Convenio 108 daba a los países de la unión, otorgando a los Estados miembros la facultad para establecer el marco regulatorio -en su derecho interno- de dichas condiciones y previsiones.

A su vez, la directiva regulaba el derecho de acceso, preveía los derechos de rectificación y cancelación de datos, e incorporaba los derechos de bloqueo y notificación a terceros -para el supuesto de que se hubiera ejercido la rectificación, supresión o

⁴⁹ Art. 1 del Convenio 108.

⁵⁰ Art. 2, inc. c, del Convenio 108.

⁵¹ Jos Dumortier, *"Aplicación de la Directiva de Protección de Datos en Bélgica"*, Universidad Pontificia Comillas, Madrid, 1996 - 1997, pág. 51/74.

bloqueo de datos y los mismos hubieran sido utilizados por un tercero-. En paralelo, dicha norma- mantenía el derecho del interesado a oponerse al tratamiento de sus datos personales y disponía la prohibición de que aquel fuera sometido a decisiones con efectos jurídicos basadas únicamente en un tratamiento automatizado⁵². Otro antecedente del art. 22 del RGPD.

Por su parte, se impuso a los Estados miembros la obligación de velar por el respeto de las medidas técnicas y de organización apropiadas para garantizar un nivel de seguridad adecuado de tratamiento de datos, fijando pautas para su determinación.

Sin embargo, cabe señalar que esta norma no contaba con sanciones severas ante el incumplimiento de sus disposiciones, ni tampoco aplicaba la extraterritorialidad de las obligaciones y sanciones contenidas en la misma.

Pasado el tiempo, ante el avance de la tecnología (creación del “big data”), la globalización y la necesidad de proteger a los consumidores frente a los recolectores de datos, el 25 enero de 2012 nace una iniciativa del Parlamento Europeo que propone una reforma de la Directiva 95/46/CE para fortalecer el derecho a la privacidad de los ciudadanos europeos y mejorar la economía digital de la región⁵³.

Luego de ciertas modificaciones al proyecto original, el 12 de marzo de 2014 el Parlamento Europeo aprobó la primera redacción del RGPD (621 votos a favor, 10 en contra y 22 abstenciones⁵⁴). El texto definitivo sería aprobado el 27 de abril de 2016 y entraría en vigor el 25 de mayo de 2018.

2.5. Antecedentes y evolución de la regulación en materia de protección de datos personales en la República Argentina. El proyecto para reformar la Ley 25.326

⁵² Elisenda Bru Cuadrada, “La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, septiembre de 2007, obtenido el 24 de abril de 2021 de <https://www.redalyc.org/pdf/788/78812861008.pdf>.

⁵³ European Data Protection Supervisor, “The History of the General Data Protection Regulation”, obtenido el 24 de abril de 2021 de https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

⁵⁴ *Ibíd.*

El surgimiento del RGPD y su innovación legal en materia de protección de datos personales hizo que diferentes países del mundo adaptaran sus legislaciones y se inspiraran en dicho reglamento.

Así, en nuestro continente se dictaron diversas regulaciones tales como la “*California Consumer Privacy Act*” en el Estado de California en Estados Unidos o la “*Lei Geral de Proteção de Dados*” en Brasil. Y otros países, como Argentina y Chile elaboraron proyectos de ley inspirados en el nuevo reglamento europeo.

En el caso de Argentina, la protección de los datos personales se encuentra regulada y garantizada por la acción de habeas data (art. 43 de la Constitución Nacional) y la Ley 25.326 (en adelante, la “LPDP”), habiendo sido esta última pionera en la región al sancionarse el 4 de octubre del 2000. Más allá que de que en su momento nació como una ley desactualizada.

Al respecto, la LPDP se basó en el modelo de la Ley Orgánica Española 5/92 de Regulación del Tratamiento Automatizado de Datos Personales de 1992 (conocida como LORTAD)⁵⁵, pero dicha ley fue derogada el 13 de septiembre de 1999 por la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

Es decir, que al momento que nuestros legisladores tomaron la LORTAD como fuente para sancionar la LPDP, la norma española ya no estaba en vigencia y es por eso que se sostiene que nuestra norma de protección de datos nació anticuada⁵⁶.

Pero sin perjuicio de ello, en su momento, la LPDP fue la más innovadora en América Latina y llevó a que Argentina sea considerada por la Unión Europea como un país con legislación adecuada en punto a la protección datos personales transferidos desde la comunidad; ello, desde el año 2003⁵⁷.

⁵⁵ Alejandra M. Gils Carbó, “*Régimen Legal de la Bases de Datos y Habeas Data*” LL, Buenos Aires, 2001, pág. 47.

⁵⁶ Pablo A. Palazzi, “*Protección de datos personales: Doctrina y Jurisprudencia*”, CETyS, Tomo 1, pág. 28.

⁵⁷ Comisión Europea, Secretaría General, Decisión de la Comisión de fecha 30/6/2003 con arreglo de la Directiva N° 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina, Bruselas, obtenido el 26 de septiembre de 2021 de <https://ec.europa.eu/transparency/regdoc/rep/3/2003/ES/3-2003-1731-ES-F1-1>

Luego de la sanción de la LPDP y con el transcurso de los años, las regulaciones contenidas en dicha norma resultaron ser insuficientes en muchos casos -en atención al avance en materia de TIC- para proteger los datos personales de los individuos en el entorno de internet. Es por ello que en el año 2016 y desde la Dirección Nacional de Protección de Datos Personales (en adelante, la “DNPDP”), se manifestó la intención de reformar la LPDP, teniendo en consideración la reciente aprobación del RGPD en Europa.

El proceso de reflexión y análisis de la reforma de la LPDP se dio en el marco del programa “Justicia 2020”, el cual consistió en una iniciativa liderada por el Ministerio de Justicia y Derechos Humanos de la Nación, mediante del cual se desarrollaron distintos proyectos de gestión gubernamental 2015-2019. Entonces, el proyecto de reforma de la LPDP fue incluido como una de las iniciativas del eje de gestión dentro del programa “Justicia 2020”.

La elaboración del proyecto tuvo dos etapas de consultas (la primera de mayo a diciembre de 2016 y la segunda realizada en febrero de 2017) en las que participaron empresas, asociaciones y cámaras que nuclean a compañías privadas en materia de tecnología, internet, comunicaciones, entre otras.

Luego de transcurrir y desarrollar el proceso consultivo, el proyecto de reforma quedó conformado por noventa y cinco (95) artículos divididos en doce (12) capítulo. El proyecto ingresó en el Congreso de la Nación a través del Senado el 20 de septiembre de 2018 y rápidamente se giró para su tratamiento a las comisiones de “Asuntos Constitucionales” y de “Derechos y Garantías”.

En principio y según las noticias de ese entonces, señalaban que tanto el Poder Ejecutivo como los senadores oficialistas esperaban que el proyecto fuera aprobado en las comisiones correspondientes y comenzara a debatirse entre finales de septiembre y principios de octubre de 2018⁵⁸. Sin embargo, dicho proyecto no fue tratado por las comisiones mencionadas en el año 2018, ni en el 2019.

⁵⁸ Véase, Télam, <https://www.telam.com.ar/notas/201809/294198-buscan-avanzar-con-un-proyecto-que-refuerza-la-proteccion-sobre-los-datos-personales.html>, recuperado el día 30 de septiembre de 2021.

El año 2019 fue un año electoral, y con el cambio de Gobierno, el proyecto no fue tratado para ser aprobado y debatirlo en el Senado. Así y al no recibir ningún tipo de tratamiento en el Congreso de la Nación, el proyecto de ley que pretendía modernizar nuestra legislación en materia de protección de datos personales perdió estado parlamentario en febrero de 2020.

Dicho proyecto fue una primera aproximación y gran intento de reformar nuestra regulación sobre datos personales de conformidad con los lineamientos del RGPD. Lamentablemente, dicha reforma no pudo llevarse adelante por cuestiones políticas. Ojalá en los próximos años se retome esta iniciativa en atención a la importancia que los datos personales tienen en nuestras vidas en la actualidad y tendrán más aún, en el futuro.

Sentado todo lo expuesto con anterioridad, en el siguiente capítulo, pasaré a analizar algunas generalidades del RGPD; tales como el alcance territorial del mismo, nuevos derechos regulados y sanciones previstas.

3. NOCIONES GENERALES DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. ANÁLISIS DEL ARTÍCULO 22

Sentados los antecedentes históricos, normativos, doctrinarios y jurisprudenciales que motivaron el surgimiento del RGPD; a continuación, expondré sobre algunas nociones generales del reglamento, tales como los nuevos derechos que establece, el alcance territorial del mismo y las sanciones que prevé.

Una vez expuestas las generalidades del RGPD, pasaré a analizar en profundidad los cuatro apartados que contiene el artículo 22.

3.1. Nociones generales

3.1.A. Los nuevos derechos previstos en el RGPD

Sin ninguna duda, el RGPD es el cambio normativo más importante en materia de protección de datos en los últimos veinte años. Actualmente, es la norma más dura en materia de protección de datos, pero a su vez, es la que mayor seguridad jurídica brinda en el mundo⁵⁹. **En este sentido y conforme lo adelantado en el capítulo 1, compañías como Microsoft han señalado que el RGPD es una regulación estricta, pero innovadora que permitirá el desarrollo en materia de privacidad⁶⁰.**

Sin embargo y más allá de que es cierto que el RGPD provocará un mayor y mejor desarrollo en materia de protección de datos personales, la implementación del reglamento podría ocasionar también efectos adversos⁶¹. Por ejemplo, la aplicación del RGPD podría (i) restringir la innovación tecnológica (ii) generar rigurosos controles sobre compañías que almacenan datos a través del blockchain; (iii) impactar

⁵⁹ “The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world” recuperado el 21 de agosto de 2021 de <https://gdpr.eu/what-is-gdpr/>.

⁶⁰ Julie Brill, “GDPR’s first anniversary: A year of progress in privacy protection”, obtenido el 21 de agosto de 2021 de <https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/>.

⁶¹ Forbes Technologies Council “15 Unexpected Consequences Of GDPR – Forbes” obtenido el 21 de agosto de 2021 de <https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=5bc3bbaa94ad>.

negativamente en pequeñas y medianas empresas que no cuenten con los recursos económicos necesarios para adaptar su funcionamiento a los lineamientos del RGPD; (iv) eliminar lentamente la provisión de servicios gratuitos que brindan las plataformas (YouTube, Facebook, Instagram, etc.)⁶² ; entre otros.

Ahora bien, no obstante los efectos positivos y/o negativos que eventualmente generará el RGPD, resulta importante destacar los nuevos derechos que dicha norma ha creado en favor de los usuarios/interesados. Estos son:

- *Derecho a estar informado: Proporciona transparencia sobre cómo son utilizados los datos personales del usuario.*
- *Derecho al acceso: Provee al usuario acceso a sus datos, a cómo son utilizados, y a cualquier información suplementaria que pueda ser utilizada juntos con sus datos.*
- *Derecho a la rectificación: Otorga el derecho al usuario de que sus datos personales sean rectificados en caso de ser incorrectos o incompletos.*
- *Derecho a ser borrado -más conocido como derecho al olvido-: Es el derecho a que los datos personales del usuario sean removidos de cualquier lugar si no existe una razón convincente para que estén almacenados.*
- *Derecho a restringir el procesamiento: Permite que los datos de los usuarios sean almacenados, pero no procesados. Por ejemplo, se puede recurrir a este derecho si el usuario sabe que existen datos erróneos de su persona almacenados en un servidor, a la espera de ser rectificados.*
- *Derecho a la portabilidad de datos: El usuario puede solicitar copias de la información almacenada sobre su persona, para utilizar en cualquier otro lugar.*

⁶² *Ibíd.*

- *Derecho a objetar: Otorga el derecho a objetar acerca del procesamiento de datos. Un ejemplo podría ser la objeción de que sus datos sean utilizados por organizaciones de marketing directo.*
- *Derecho sobre la toma de decisiones y creación de perfiles automáticos -el derecho que aquí nos interesa-: Permite al usuario objetar sobre la toma de decisiones automáticas que se hagan sobre sus datos personales. “Automáticas” se refiere a sin intervención humana. Por ejemplo, la definición de determinados hábitos de compra online, en función a comportamientos previos.*

Al respecto, estos derechos otorgan a los interesados nuevas facultades y/o prerrogativas para proteger sus datos personales, y para que, en el eventual caso de estar sufriendo un daño y/o perjuicio originado por el tratamiento de sus datos, se disponga la eliminación o rectificación de los mismos.

En términos generales, la nueva normativa europea en materia de protección de datos ha sido creada para proteger fuertemente los derechos de los usuarios frente al avance tecnológico -y en particular, frente al almacenamiento y utilización de los datos personales de los usuarios- que viene ocurriendo en los últimos años.

Pero sin perjuicio de la finalidad “pro-usuario” del RGPD, su aplicación también podría generar un abuso de posición dominante de ciertos responsables⁶³ y/o encargados⁶⁴ del tratamiento⁶⁵, y que las pequeñas y medianas empresas no puedan ingresar en el mercado de datos⁶⁶.

⁶³ El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento de los datos personales (conf. art. 4, apartado 7).

⁶⁴ El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (conf. art. 4, apartado 8).

⁶⁵ 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*, Vol 8, No 1, 2017), pág. 8.

⁶⁶ El mercado de datos es el lugar en el que los agentes pueden comprar y vender datos a través de medios electrónicos. Concepto sobre el que volveré más adelante.

Es por ello que si bien el RGPD es una norma fundamental que garantizará muchos derechos de los usuarios y beneficiará su posición frente a los responsables y/o encargados del tratamiento, no es menos cierto que la aplicación de algunos artículos de dicha norma podría generar ciertas ineficiencias económicas.

Sentados los nuevos derechos promovidos por el RGPD, pasaré a explicar el alcance territorial del mismo.

3.1.B. El alcance territorial del RGPD

El artículo 3 del RGPD establece tres criterios y pautas para determinar el alcance territorial de las normas del reglamento con respecto al tratamiento de datos realizado por el responsable y/o encargado y/u organismo público.

Al respecto, resulta importante señalar que para aplicar el RGPD de conformidad con los criterios establecidos para su alcance territorial, es sumamente importante analizar caso por caso, teniendo en cuenta ciertas cuestiones como por ejemplo, la finalidad del tratamiento, la existencia -o no- de un establecimiento dentro de la Unión Europea, el lugar de residencia de los interesados, entre otros.

Este artículo está dividido en tres apartados; el primero fija el criterio del “*establecimiento*”, el segundo establece el criterio de la “*selección de destinatarios*” - también conocido como *targeting*- y, el tercer y último criterio es el de “*aplicación del RGPD en virtud del Derecho Internacional Público*”. Es decir, que estos tres apartados en su conjunto cubren -de manera amplia y completa- las distintas situaciones y/o casos a los que se les va a aplicar el RGPD. Veamos a continuación, estos tres criterios:

 Criterio del establecimiento: el apartado 1 del artículo 3 del RGPD establece que sus normas se aplicarán al tratamiento de datos personales realizado por un responsable y/o encargado en el contexto de actividades de un establecimiento de dicho

responsable y/o encargado que se encuentra en la Unión Europea, independientemente de que el tratamiento de datos se realice o no en el territorio de la Unión⁶⁷.

En términos simples, esto quiere decir que, las normas del RGPD se van a aplicar al tratamiento de datos que se realice dentro o fuera del territorio de la Unión Europea teniendo en cuenta que el responsable y/o encargado del tratamiento deben tener un establecimiento (oficina) dentro del territorio de la Unión. A continuación, se ilustra dicha situación con un ejemplo brindado por el Comité Europeo de Protección de Datos (en adelante, el “CEPD”)⁶⁸ en la Directrices 3/2018 relativas al ámbito territorial del RGPD.

Ejemplo 2: un sitio web de comercio electrónico es explotado por una empresa radicada en China. Las actividades de tratamiento de datos personales de la empresa se llevan a cabo exclusivamente en China. La empresa china ha establecido una oficina europea en Berlín para dirigir y llevar a cabo campañas de comercialización y prospección comercial hacia los mercados de la UE.

En este caso, puede considerarse que las actividades de la oficina europea de Berlín están indisolublemente ligadas al tratamiento de datos personales llevado a cabo por el sitio web de comercio electrónico chino, en la medida en que la campaña de comercialización y prospección comercial destinada a los mercados de la UE sirve especialmente para rentabilizar el servicio ofrecido por el sitio web de comercio electrónico. El tratamiento de datos personales por parte de la empresa china en relación con las ventas en la UE está indisolublemente ligado a las actividades de la oficina europea de Berlín en relación con la campaña de comercialización y prospección comercial hacia el mercado de la UE. El tratamiento de datos personales por parte de la empresa china en relación con las ventas en la UE puede, por tanto, considerarse realizado en el contexto de las actividades de la oficina europea, como establecimiento situado en la Unión. Por lo tanto, esta operación de tratamiento por parte de la empresa china estará sujeta a las disposiciones del RGPD en virtud de su artículo 3, apartado 1.

✚ Criterio de la selección de destinatarios: el apartado 2 del artículo 3 dispone que la inexistencia de un establecimiento del responsable y/o encargado en el territorio de la Unión Europea, no implica que el tratamiento de datos personales realizados en un tercer país quede excluido de la aplicación del RGPD.

⁶⁷ Comité Europeo de Protección de Datos, “Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3)” 12/11/2019, pág. 5, obtenido el 29 de agosto de 2021 de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf.

⁶⁸ Comité Europeo de Protección de Datos, “Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3)” 12/11/2019, pág. 9, obtenido el 29 de agosto de 2021 de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf.

Reitero, para determinar la aplicación territorial del RGPD, siempre será necesario evaluar el caso concreto para determinar si se le debe -o no- aplicar las normas de dicho reglamento.

Pues bien, el apartado 2 del artículo 3 se aplicará siempre que el tratamiento de datos esté relacionado con (i) la oferta de bienes y servicios a los interesados de la Unión Europea, con independencia de si se requiere un pago por parte del interesado; o bien, con (ii) el control del comportamiento de los interesados, siempre que se realice en el territorio de la Unión.

Ejemplo del punto (i)⁶⁹:

Ejemplo 14: un sitio web, basado y gestionado en Turquía, ofrece servicios para la creación, la edición, la impresión y el envío de álbumes de fotos familiares. El sitio web está disponible en inglés, francés, neerlandés y alemán, y los pagos pueden efectuarse en euros. El sitio web indica que los álbumes fotográficos solo pueden entregarse por correo postal en Francia, los países del Benelux y Alemania.

En este caso, es evidente que la creación, la edición y la impresión de álbumes de fotos familiares personalizados constituyen un servicio en el sentido del Derecho de la UE. El hecho de que el sitio web esté disponible en cuatro lenguas de la UE y de que los álbumes de fotografías puedan entregarse por correo postal en seis Estados miembros de la UE demuestra que el sitio web turco tiene la intención de ofrecer sus servicios a particulares que residen en la Unión.

En consecuencia, es evidente que el tratamiento realizado por el sitio web turco, como responsable del tratamiento de los datos, se refiere a la oferta de un servicio a interesados en la Unión y está, por tanto, sujeto a las obligaciones y disposiciones del RGPD, de conformidad con el artículo 3, apartado 2, letra a).

Por su parte y con relación al punto (ii), cabe señalar que son catalogadas como actividades de control a: la publicidad comportamental, actividades de geolocalización con fines de comercialización, estudios de comportamientos basados en perfiles individuales, seguimiento sobre el estado de salud de una persona.

Ejemplo del punto (ii)⁷⁰:

Ejemplo 17: una empresa de consultoría minorista establecida en los Estados Unidos ofrece asesoramiento sobre la distribución al por menor a un centro comercial de Francia, sobre la base de un análisis de los movimientos de los clientes por todo el centro, registrados mediante el seguimiento wifi.

⁶⁹ *Ibíd.*

⁷⁰ *Ibíd.*

El análisis de los movimientos de los clientes dentro del centro a través del seguimiento wifi constituirá el control del comportamiento de los particulares. En este caso, el comportamiento de los interesados tiene lugar en la Unión, ya que el centro comercial está situado en Francia. La empresa de consultoría, como responsable del tratamiento de los datos, está, por tanto, sujeta al RGPD en lo que respecta al tratamiento de estos datos con este fin, de conformidad con el artículo 3, apartado 2, letra b).

De conformidad con el artículo 27, el responsable del tratamiento deberá designar un representante en la Unión.

✚ Criterio de aplicación del RGPD en virtud del Derecho Internacional Público: este criterio, establecido por el apartado 3 del artículo 3 del RGPD, se aplica al tratamiento de datos personales que realizan las embajadas y consulados de los países de la Unión Europea que están situados, lógicamente, en otros Estados. Tal como se ilustra con el siguiente ejemplo⁷¹:

Ejemplo 22: el consulado de los Países Bajos en Kingston (Jamaica) abre un proceso de solicitud en línea para la contratación de personal local con el fin de reforzar su administración.

Aunque el consulado de los Países Bajos en Kingston (Jamaica) no está establecido en la Unión, el hecho de que se trate de una oficina consular de un país de la UE donde se aplica la legislación de un Estado miembro en virtud del Derecho internacional público implica que el RGPD es aplicable a su tratamiento de datos personales, de conformidad con el artículo 3, apartado 3.

Sentados estos tres criterios, resulta importante destacar que el artículo 3 del RGPD ha marcado una importante evolución de la legislación en materia de protección de datos personales en punto al alcance territorial de las normas contenidas en el mismo, por cuanto abarca una gran cantidad de supuestos fácticos a los cuales se aplicarán las normas de dicho reglamento, debiendo siempre -reitero una vez más- evaluarse las circunstancias particulares del caso concreto.

Aclarados los criterios y supuestos aplicables al alcance territorial del RGPD, pasaré a mencionar las sanciones administrativas previstas ante el incumplimiento de dicho reglamento.

3.1.C. Sanciones

El RGPD ha realizado otro cambio importante sobre las sanciones previstas para el caso de que los responsables y/o encargados del tratamiento de datos incumplan las

⁷¹ *Ibíd.*

normas del reglamento. Dichas multas administrativas se encuentran previstas en el artículo 83 y deben ser efectivas, proporcionadas con la infracción que se cometió y disuasorias de la conducta lesiva.

Así, el cambio más significativo está dado por el aumento de los montos de las sanciones administrativas. Al respecto, “...el art. 83 en sus apartados 4 y 5, que sin hacer mención específica a cuantías mínimas, prevé la posibilidad de sancionar las infracciones cometidas con respecto al tratamiento de datos de carácter personal con multas administrativas de 10.000.000 o 20.000.000 de euros, o en el caso de que se trate de una empresa, de una cuantía equivalente al 2% o al 4% como máximo del volumen de negocio anual global del ejercicio financiero anterior, optándose por la de mayor cuantía”⁷².

A su vez, el RGPD permite a los países de la Unión Europea legislar normas en materia penal para sancionar infracciones del reglamento, que pueden implicar la privación de las ganancias obtenidas del tratamiento de datos realizado.

Por su parte, el RGPD introduce una figura novedosa que es la posibilidad de multar a los organismos de la administración pública. En este sentido, el apartado 7 del artículo 83 prevé que las sanciones administrativas -y económicas- sean impuestas tanto a las empresas privadas, como a las autoridades y organismos públicos.

Ahora bien, si bien esta regulación equipara a las organizaciones privadas con las organizaciones y autoridades estatales -en punto a la imposición de sanciones-, parece improbable que los Estados miembros de la Unión sancionen a sus propios organismos, con el impacto económico negativo que ello podría causar en las arcas públicas.

No hay que dejar de señalar que para aplicar las sanciones previstas en el artículo 83, la autoridad de aplicación deberá evaluar el caso concreto para determinar si hubo -o no- una infracción a las disposiciones del reglamento.

⁷² Sonia Vásquez y Javier de Miguel, “Nuevo Régimen Sancionador De Protección De Datos”, Revista Economist & Jurist, obtenido el 29 de agosto de 2021 de <https://ecija.com/wp-content/uploads/2017/06/Sanciones-RGPD.pdf>.

Sentado lo anterior, resulta importante destacar que el RGPD ha introducido nuevas consideraciones en la imposición de sanciones administrativas que llevará a las distintas organizaciones de la comunidad (privadas o públicas) a adoptar los recaudos necesarios y cumplir con las directrices del reglamento. En caso contrario, estarán sujetas a las consecuencias y sanciones gravosas que el RGPD ha regulado para los eventuales infractores.

Explicadas algunas de las nociones generales del RGPD, a continuación, analizaré en detalle los cuatro apartados contenidos en el artículo 22 del mencionado reglamento.

3.2. El artículo 22 del RGPD: Decisiones individuales automatizadas, incluida la elaboración de perfiles

3.2.A. El mencionado artículo contempla lo siguiente:

- 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.

3.2.B. En el **primer apartado**, se dispuso lo central del artículo bajo análisis; que es que todo interesado tiene el derecho a no ser objeto de decisiones basadas únicamente en procesos automatizados de toma de decisiones.

Este proceso consiste en tomar decisiones a través de medios automatizados - que utilizan el big data y machine learning- y sin que participe una persona humana. Esas decisiones se toman con fundamento/apoyo en la información (datos fácticos) que se recolecta de las personas y en los perfiles que sobre ellas se crean⁷³.

Un ejemplo de ello son los procesos de toma de decisiones que adoptan las fintechs para otorgar créditos a sus clientes. Estas entidades recopilan los datos personales de las actividades online y offline de sus clientes, y con toda esa información evalúan la solvencia del consumidor y determinan su calificación crediticia para aprobar -o no- un crédito.

La novedad regulatoria que trajo el artículo 22 fue la inclusión de los perfiles individuales (también conocido como “*profiling*”) que se crean sobre los interesados y respecto de los cuales se extrae información para tomar decisiones. En este punto es importante señalar que el derecho de no ser objeto de una decisión basada únicamente en

⁷³ Information Commissioner’s Office, “*What is automated decision making including profiling?*” recuperado de <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>, el 2 de octubre de 2021.

un proceso automatizado ya estaba contemplado en la Directiva 95/46/CE, pero en dicha regulación no se preveía la elaboración de perfiles.

Básicamente, de los perfiles elaborados, se extraen datos personales de los interesados para evaluar y predecir aspectos relativos al comportamiento, situación económica, salud, preferencias personales, intereses y ubicación.

El Grupo de Trabajo del artículo 29 establece que para que sea aplicable el RGPD a la elaboración de perfiles, se deben reunir tres recaudos: (i) debe ser una forma automatizada de tratamiento de datos (ii) debe ser llevada a cabo respecto de información de personas humanas y (iii) el objeto de la elaboración del perfil debe ser el de “evaluar aspectos personales” de una persona humana.

En este sentido, ha sido un gran acierto incorporar la elaboración de perfiles en el artículo 22 ya que la misma será muy relevante en los próximos años con el avance de la tecnología y deberá estar en la órbita de dicho reglamento para tener un mejor control de su utilización.

Por otro lado y en punto a las “decisiones que producen efectos jurídicos en el interesado o que lo afectan significativamente y de modo similar”, el Grupo de Trabajo del artículo 29 señaló que para que la decisión tenga efectos jurídicos, debe afectar derechos inherentes del interesado tales como la libertad de asociación, votar y/o reclamar judicialmente; o bien, afectar el estado legal de una persona o sus derechos en un contrato⁷⁴.

En paralelo, las decisiones que afectan al interesado significativamente y de manera similar son aquellas que, sin producir efectos legales, puedan ser parte del ámbito de aplicación del artículo 22 debido al impacto que genera en el interesado⁷⁵. Ejemplo de ellas pueden ser: (i) circunstancias que puedan afectar las condiciones financieras de una persona, como su calificación para ser beneficiario de un crédito; (ii) que afecten el

⁷⁴ Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, obtenido de https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 el día 2 de octubre de 2021.

⁷⁵ *Ibíd.*

acceso a la salud de un interesado; y/o (iii) que nieguen el acceso de una persona a la educación, como las admisiones en la universidad⁷⁶.

3.2.C. En el **segundo apartado**, se prevén las tres excepciones a la regla establecida en el apartado 1; estas son, necesidad contractual, autorización por normativa europea o nacional y/o expreso consentimiento del interesado.

- Necesidad contractual:

Para que esta excepción sea aplicable, el responsable debe demostrar que para la celebración o ejecución de un contrato es necesaria la toma de decisiones automatizada y que no es posible utilizar otro medio menos invasivo de la privacidad. Así, esta excepción impediría que el responsable del tratamiento alegue la mera existencia de la relación contractual con el interesado para exceptuarse de cumplir con el artículo 22, apartado 1⁷⁷.

Por ejemplo, a raíz de la publicación de un anuncio de trabajo para una posición vacante en una empresa, miles de personas han aplicado para el puesto. Debido a la gran cantidad de aplicaciones recibidas, la empresa (que sería el responsable del tratamiento) debe demostrar que no es posible encontrar al candidato adecuado para la posición sin utilizar un medio de tratamiento automatizado de datos, que analice los datos de los postulantes. Entonces, en este caso, si sería necesaria la utilización del tratamiento y toma de decisiones automatizadas para reducir la lista de posibles candidatos para el puesto de trabajo vacante.

- Autorización por normativa europea o nacional:

La legislación europea o nacional de cada país puede autorizar la toma de decisiones automatizadas en supuestos determinados. En particular, cuando existe una contraposición con una norma local que pueda alterar la armonización pretendida por el RGPD.

⁷⁶ *Ibíd.*

⁷⁷ Mendoza, I. y Bygrave, L.A. “*The right not to be subject to automated decision based on profiling. In EU Internet Law: Regulation and Enforcement*” pág. 77-79.

- Expreso consentimiento del interesado:

El tratamiento automatizado de datos también será posible si el interesado brinda su consentimiento expreso; esto implica que el interesado debe realizar una declaración expresa y concreta de voluntad de que sus datos sean tratados por dichos medios.

3.2.D. El tercer apartado impone al responsable del tratamiento la obligación de adoptar medidas de protección cuando se realice un tratamiento automatizado de datos por necesidad contractual y/o por consentimiento expreso del interesado. Entonces, este apartado establece que como mínimo -sería una suerte de medida de protección- el interesado tiene derecho a que una persona humana intervenga en el tratamiento, a expresar su punto de vista y/o a impugnar la decisión.

Como se verá más adelante, este apartado podría generar una barrera legal a la entrada, **impidiendo el ingreso al mercado de datos europeo de empresas que no cuentan con los recursos suficientes para contratar a la gran cantidad de trabajadores que se necesitaría para controlar e intervenir en el tratamiento de datos personales y la toma de decisiones automatizada.**

Volviendo con el análisis del tercer apartado, el interesado tiene el derecho de que una persona humana tome intervención y que la decisión deje de ser únicamente automática; y en paralelo, el interesado también tiene la facultad de exponer su opinión e impugnar la decisión. Sin embargo, el RGPD no determina las consecuencias legales del ejercicio de estos derechos, ni tampoco determina quién debe dar respuesta a la eventual impugnación que realicen los interesados⁷⁸.

3.2.E. Finalmente, el cuarto apartado prohíbe el tratamiento automatizado de las categorías especiales de datos personales contempladas en el artículo 9.1. del RGPD. Estas categorías especiales son aquellas vinculadas con el origen étnico o racial, opiniones políticas, creencias religiosas o filosóficas, afiliación sindical, datos genéticos,

⁷⁸ Brkan. M. “Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond”, SSRN, recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901 el 3 de octubre de 2021.

datos biométricos, datos relativos a la salud, a la vida sexual u orientación sexual de una persona.

Dicha prohibición en el tratamiento deberá considerar a su vez las excepciones de que el interesado haya dado su consentimiento expreso (artículo 9.2. inc. a del RGPD) o que el tratamiento automatizado sea necesario por razones de orden público (artículo 9.2. inc. g del RGPD) y siempre que se tomen las medidas necesarias para proteger al interesado. No obstante y a diferencia del tercer apartado, no se detallan las medidas a adoptar.

Analizado los cuatro apartados del artículo 22, pasaré a exponer sobre sobre la utilidad y usos que los procesos automatizados de toma de decisiones pueden tener en ciertas industrias y/o campos de estudios.

4. LA UTILIDAD DE LOS PROCESOS AUTOMATIZADOS DE TOMA DE DECISIONES PARA EL DESARROLLO DE CIERTAS INDUSTRIAS Y CAMPOS DE ESTUDIOS. LAS RESTRICCIONES E INEFICIENCIAS ECONÓMICAS QUE PODRÍA GENERAR EL ART. 22 DEL RGPD

Analizado el artículo 22 del RGPD, veremos que ciertas industrias y campos de estudios dependen en gran medida de los procesos automatizados de toma de decisiones para su desarrollo, y para mejorar la calidad de los bienes y servicios que proveen a los consumidores. En este capítulo expondré distintos ejemplos de tecnologías -basadas en big data y machine learning-, cuyo desarrollo depende de los procesos automatizados de toma de decisiones y mencionaré los beneficios que las mismas conllevan en términos de eficiencia y reducción de costos.

Luego de ello, pasaré a exponer cómo la regulación prevista en el artículo mencionado podría causar restricciones económicas en el mercado de datos y la libre competencia, analizando tres posibles ineficiencias; estas son, (i) creación de una barrera legal a la entrada; (ii) desincentivo para innovar y desarrollar nuevas tecnologías y (iii) mayor concentración en el mercado de datos.

4.1. La utilidad e importancia de los procesos automatizados de toma de decisiones. Sus beneficios sobre los consumidores

4.1.A. Los procesos automatizados de toma de decisiones son el motor para el desarrollo y evolución de muchas industrias y campos de estudios. Más aún, considerando el avance de la inteligencia artificial en los últimos años. Por eso, este trabajo busca mostrar que estos procesos automatizados son de gran importancia para aumentar el bienestar agregado de los interesados (consumidores de bienes y servicios) y que la regulación prevista en el artículo 22 del RGPD podría ser contraproducente de esos mismos derechos que intenta proteger.

Así, la regulación prevista en el artículo bajo análisis, podría desincentivar a que ciertas industrias desarrollen ciertos bienes y servicios que se valen de la recolección de

datos personales -y que incrementan el bienestar de los consumidores-; entonces, y como veremos a continuación, el beneficio que los interesados tendrían si no se hubiera regulado el artículo 22 -o por lo menos si estuviera redactado de otra manera- sería mayor que el que recibirían por la aplicación de dicha norma.

Sentado lo anterior, a continuación me expediré sobre los beneficios que la toma de decisiones automatizada genera en industrias como la financiera, automotriz y construcción; así como en campos de estudios como la medicina y/o los recursos humanos.

Veamos:

 **Industria financiera:** En el mundo financiero se está produciendo una revolución con las -tan de moda- Fintechs; y **la recolección y tratamiento de datos personales resulta importante no solo en materia de innovación, sino también para facilitar el acceso al crédito e incluir financieramente a aquellas personas que quedaron apartadas por el sistema tradicional.**

Teniendo en cuenta las ineficiencias actuales que deja la banca tradicional, las Fintechs aprovechan dicha situación y mediante el análisis del big data y las técnicas de machine learning (recolección de datos personales de los usuarios a partir de búsquedas de internet, redes sociales, aplicaciones, entre otros), explotan cada vez más las “huellas digitales” que dejan las personas excluidas del sistema financiero; y con ello, promueven la bancarización de las mismas.

Por ejemplo, en Argentina existe un gran porcentaje (80%) de la población de clase media con ingresos estables que si bien puede tener caja de ahorro y una tarjeta de débito asociada, no se encuentra bancarizada⁷⁹. Razón por la cual, no se le permite tener acceso a productos de crédito como tarjetas, descubiertos, préstamos y/o chequeras. A la vez, al no tener dichas personas un historial formal de comportamiento de crédito en la banca tradicional -que utiliza modelos de “scoring” basados en el comportamiento crediticio o financiero-, no se las considera aptas de ser asistidas crediticiamente. Por lo

⁷⁹ BCRA y CAF. Encuesta de medición de capacidades financieras en Argentina, 2017.

tanto, este gran número de personas no bancarizadas se encuentra en un estado de exclusión financiera.

Así, mediante el desarrollo de un scoring que pretende adoptar un enfoque más integral de la información recolectada de los usuarios -no solo la información tradicional que utilizan las entidades financieras-, se extraen datos de las actividades online y offline de los consumidores. Esto es, cada vez que las personas no bancarizadas hacen una llamada, navegan por internet y/o utilizan las redes sociales a través de sus smartphones, dejan sus “huellas digitales”.

Toda esa información que los usuarios dejan en sus “huellas digitales”, es recolectada por las Fintech y se utiliza para evaluar el riesgo del consumidor y determinar la solvencia de los actores no bancarizados y excluidos del sistema.

En este sentido, un score de crédito mediante la aplicación del big data y técnicas de machine learning puede basar la decisión de crédito analizando diferentes variables como “dónde compran” y “qué compran” las personas, la actividad que tienen en sus redes sociales y otros factores que no están intrínsecamente relacionados con la solvencia crediticia del individuo; y en virtud de este score, los prestamistas pueden usar el resultado de su calificación crediticia para ofrecer crédito no garantizado, de corto plazo y a un costo mucho menor que los préstamos de la banca tradicional.

En virtud de lo anterior, vemos cómo se utiliza y aprovecha la recolección de datos de los usuarios para definir el perfil de eventuales prestatarios no bancarizados; y con ello, analizar la posibilidad de crear un score “inclusivo” que permita a dichas personas acceder a un crédito, **el que se otorgará a través de un proceso automatizado de decisiones.**

Como vemos, la recolección de datos de los interesados y la toma de decisiones automatizadas son importantísimas para avanzar en la inclusión financiera de personas que fueron dejadas de lado por el sistema tradicional; las que si tendrían acceso al crédito o a prestaciones como una tarjeta de crédito, podrían aumentar su bienestar y calidad de vida.

✚ **Industria automotriz:** En esta industria, y en particular, con relación a los vehículos autónomos, **la recolección y tratamiento de datos personales es relevante para brindar mayor seguridad y asistencia a los conductores mientras manejan.**

Respecto de la industria de vehículos autónomos, se estima que la misma podría generar mundialmente alrededor de siete trillones de dólares para el año 2050, así como también prevendrá la muerte de 585.000 personas entre los años 2035 y 2045; ello, considerando que el 94% de los accidentes viales son causados por el error humano⁸⁰; por lo que vemos que en un futuro esta industria tendrá mucha relevancia en nuestro mundo, no solo en lo económico, sino para evitar la muerte y/o daños/lesiones de miles de personas.

La recolección de datos personales de las personas que manejan los vehículos autónomos puede servir para desarrollar tecnologías que permitan medir el nivel de peligrosidad de cada conductor (riesgo de manejo).

Así y si bien aún no contamos con la tecnología suficiente para tener un vehículo 100% autónomo, la recopilación de información vinculada con las características personales del conductor resulta esencial para alcanzar dicha meta⁸¹. Entonces, para mejorar la seguridad y asistencia del vehículo al conductor, es necesario que sensores dentro del auto recolecten información de los movimientos corporales y expresiones faciales para advertir cuando, por ejemplo, el conductor se queda dormido mientras maneja.

A su vez, dichos sensores podrían detectar las preferencias del conductor en punto a las rutas/caminos que elige frecuentemente; así como también la velocidad a la

⁸⁰ Roger Lanctot, “*Accelerating the Future: The Economic Impact of the Emerging Passenger Economy*”, Strategy Analytics, Intel, pág- 5, recuperado el 6 de noviembre de 2021 del sitio web 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

⁸¹ 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, obtenido el 6/11/2021 del sitio web <https://hcai.mit.edu/avt/>

que viaja de manera periódica; información que es relevante para que los conductores tengan una mejor experiencia al ser transportados⁸².

Sin esta recolección y tratamiento de datos personales, sería más difícil que los sistemas se adaptaran personalmente a las necesidades y preferencias de los consumidores. Asimismo, es evidente que la obtención de esta información es clave para mejorar el bienestar y, por sobre todo, la vida de los interesados; dado que a partir de la información obtenida por el vehículo autónomo, se podría salvar al propio conductor de un error que puede costarle la vida.

Sentado ello, vemos que en esta industria también resulta sumamente relevante el proceso de recolección de datos y toma de decisiones automatizadas, no solo para mejorar la innovación y competitividad de los productos, sino para incrementar el bienestar de los usuarios y consumidores.

✚ **Industria de la construcción:** La recolección de datos y procesos automatizados de decisión también se da en la construcción con las casas automatizadas, llamadas “*Home Automation*”.

*“Una casa automatizada es aquella en la que cada artefacto puede ser manejado de manera remota desde cualquier lugar que se tenga acceso a internet”*⁸³ (traducción propia).

A su vez, y como este tipo de casas están integradas con inteligencia artificial, el sistema va recopilando y tratando datos, y adapta ciertas funcionalidades de la casa a las características personales de quienes habitan la misma.

Estos sistemas utilizan la recolección de datos personales y los procesos de toma de decisión automatizada para activar o desactivar funciones de la casa como por ejemplo, la energía (luces). Así, en una casa integrada con inteligencia artificial hay

⁸² Chelsey Colbert, “*Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles*”, Universidad de Stanford, obtenido el 6 de noviembre de 2021 del sitio <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>.

⁸³ Sandeep Kumar and Mohammed Abdul Qadeer, “*Application of AI in Home Automation*”, IACSIT International Journal of Engineering and Technology, Vol. 4, No. 6, December 2012.

sensores que detectan la presencia de las personas en el lugar en donde está la luz prendida, por lo que si alguien se olvida de apagar la luz, la casa automáticamente apaga la misma; haciendo más eficiente el consumo de energía⁸⁴.

En idéntico sentido, el sistema inteligente integrado a la casa recolecta la información de la temperatura externa durante el transcurso del año y, dependiendo de las preferencias de las personas que la habitan, establece la temperatura interna de la casa.

También se utiliza la recolección de datos y los procesos de toma de decisiones para brindar mayor seguridad a la casa. Al respecto, primero, los sensores del sistema de seguridad advierten una posible amenaza; luego, el sistema analiza -a partir de los datos recolectados- si esa amenaza es -o no- real. Si el sistema detecta que la amenaza es real, dispara la alerta tanto a los que habitan la casa, como a la policía o seguridad privada del lugar.

Entonces, vemos que en el caso de la construcción, los procesos automatizados de toma de decisiones resultan apropiados para hacer más eficiente el consumo de energía, aumentar el confort de las personas que habitan la casa y mantener la seguridad del lugar ante eventuales amenazas.

 **Campo de la medicina:** En lo que respecta a la medicina, **la recolección de datos personales y procesos automatizados de toma de decisiones también son una herramienta fundamental para diagnosticar y prevenir enfermedades futuras en pacientes.**

Al respecto, los diagnósticos médicos son actividades complejas que requieren el análisis de una serie de estudios y antecedentes patológicos del paciente, por lo que deben tomarse grandes recaudos para poder diagnosticar con precisión la enfermedad del mismo. En este sentido, actualmente se desarrollan sistemas integrados con inteligencia artificial que podrían inclusive mejorar la precisión de esa difícil tarea que es diagnosticar la enfermedad de un paciente.

⁸⁴ Ibid.

En efecto, investigadores de Google diseñaron un algoritmo que puede detectar con gran precisión (98%) la retinopatía diabética (que es el daño en los vasos sanguíneos del tejido ubicado en la retina)⁸⁵. Por otro lado, en el hospital “Moorfields Eye” de Londres diseñaron un algoritmo que puede predecir más de 50 enfermedades oculares también con un nivel de precisión alta (94%)⁸⁶. Y a su vez en China, en el hospital de Sichuan, se desarrolló un software que incrementó el porcentaje de detección del cáncer de colon (del 20% al 29%)⁸⁷.

Es indudable que gracias a la recolección de datos personales de los pacientes y al desarrollo de algoritmos que toman decisiones basadas en la evidencia y similitud de casos -como los ejemplos anteriores que vimos-, se puede aumentar la expectativa de vida y salud de las personas.

✚ **Campo de los recursos humanos:** Muchas veces las organizaciones privadas y/o públicas incurren en altos costos de transacción para encontrar a un candidato que se ajuste a la posición de trabajo ofrecida. La selección de un candidato entre varios postulantes insume mucho tiempo, recursos económicos y expectativas, haciéndose largo el proceso de selección cuando a veces la posición requiere ser cubierta a la brevedad. Aquí, **la recolección de datos personales (recopilación de currículums vitae) y el diseño de algoritmos de selección se vuelve vital para hacer más eficiente el proceso y reducir los costos de transacción.**

Los procesos automatizados de toma de decisiones pueden generar grandes ganancias en eficiencia en los recursos humanos; así, por ejemplo, mediante el uso de algoritmos se pueden automatizar tareas repetitivas y que insumen tiempo, como “...*la administración de compensación y beneficios, las preguntas de empleados sobre procedimientos y políticas o el análisis de los currículos.*”⁸⁸.

⁸⁵ Julia Belluz, “3 ways AI is already changing medicine”, recuperado el 7 de noviembre de 2021 del sitio web <https://www.vox.com/science-and-health/2019/3/15/18264314/ai-artificial-intelligence-deep-medicine-health-care>.

⁸⁶ *Ibíd.*

⁸⁷ *Ibíd.*

⁸⁸ Guido Stein, “*La inteligencia artificial en la selección de personas*”, obtenido el día 7 de noviembre de 2021 del sitio <https://www.harvard-deusto.com/la-inteligencia-artificial-en-la-seleccion-de-personas>.

A su vez, estos procesos integrados con inteligencia artificial, pueden generar una mejor captación de talento, habida cuenta que permiten comparar las capacidades de los postulantes con el desempeño de los mejores empleados que esas organizaciones tienen.

En paralelo, los algoritmos pueden analizar de manera más rápida y precisa los curriculums vitae recibidos para la posición. En promedio, el personal de recursos humanos insume aproximadamente un tercio de la semana de trabajo seleccionando candidatos⁸⁹; por lo que los procesos automatizados de toma de decisiones ayudarían a los reclutadores a tener más tiempo en tareas más importantes en el proceso de selección; por ejemplo, tener entrevistas.

Sentado lo expuesto, es evidente que los motores de inteligencia artificial pueden agilizar el proceso de selección de personal, generar ganancias de eficiencia y eliminar tareas repetitivas que insumen tiempo valioso de los reclutadores.

Una vez más, vemos que la recolección de datos personales (de los candidatos) y los procesos automatizados de toma de decisiones son altamente positivos para el desarrollo, en este caso, de los recursos humanos.

4.1.B. Llegado a este punto y habiendo analizado ciertos casos en que los procesos automatizados de toma de decisiones resultan esenciales para el desarrollo de nuevas tecnologías y para mejorar la calidad de los bienes y servicios que se brindan a los usuarios, es necesario señalar que son evidentes las ventajas que representan estos sistemas en términos de eficiencia y reducción de costos de transacción; y es por ello que la regulación prevista en el artículo 22 del RGPD debería ser modificada; para promover más innovación con estos procesos, en lugar de limitarlos como inspira el actual texto normativo.

En efecto, ha sido la propia Comisión Europea la que ha reconocido el impacto positivo que estos procesos automatizados de toma de decisiones pueden tener en los consumidores al sostener que:

⁸⁹ *Ibíd.*

- Las aplicaciones basadas en machine-learning permiten que los consumidores puedan ahorrar tiempos. La aspiradora automática o el sistema de auto regado (los dos existen actualmente) liberan a los consumidores del tiempo que insume realizar las tareas del hogar para que puedan utilizar ese tiempo para otra cosa⁹⁰.
- Las aplicaciones basadas en machine-learning también pueden hacer que ciertos dispositivos electrónicos entreguen productos hechos a medida o presten servicios⁹¹.
- Las aplicaciones que traducen voz a texto y viceversa pueden ayudar a personas con discapacidades (por ejemplo, personas sordas) y simplificar su vida (existen actualmente)⁹².
- Los sistemas de machine-learning e integradas en productos o servicios ofrecen el potencial de optimizar el uso de energía, aprovechar precios bajos o comparar fácilmente ofertas complejas. Estas aplicaciones pueden incrementar la eficiencia y sustentabilidad de los servicios; por ejemplo, si detectan que no hay ninguna persona en la casa, pueden pasar automáticamente al modo de ahorro de energía⁹³.
- El machine-learning puede mejorar el trabajo de las organizaciones de consumidores ya sea monitoreando los precios en tiempo real, lo que permite elegir una mejor oferta⁹⁴.
- Las entidades regulatorias pueden valerse de aplicaciones basadas en machine-learning para detectar cláusulas abusivas en contratos predispuestos; alertar de ello a los consumidores y sancionar a los proveedores con las multas correspondientes⁹⁵.

⁹⁰ 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*”, pág. 11, 16 de mayo de 2018, recuperado el día 13 de noviembre de 2021 del sitio https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf

⁹¹ Ibid.

⁹² Ibid.

⁹³ Ibid.

⁹⁴ Ibid.

⁹⁵ Ibid.

En paralelo, la Comisión Europea también reconoce que la tecnología reduce costos de transacción, permitiendo un intercambio más eficiente de la información trasladada de un responsable a otro⁹⁶.

Así las cosas, no hay duda que la recolección de datos personales y los procesos automatizados de toma de decisiones son claves para aumentar el bienestar de los consumidores -y que sus efectos son altamente positivos-, por lo que los términos del artículo 22 del RGPD deberían ser modificados para que estas tecnologías sigan expandiéndose y continúen mejorando la prestación de bienes y servicios.

Habiendo ponderado la importancia y beneficios que los procesos automatizados de toma de decisiones tienen respecto de ciertas industrias, campos de estudios y, por sobre todo, en los consumidores, a continuación pasaré a exponer sobre las restricciones económicas en el mercado de datos y la libre competencia que podría causar la regulación del artículo 22 del RGPD.

En particular, analizaré tres posibles ineficiencias; estas son, (i) creación de una barrera legal a la entrada; (ii) desincentivo para innovar y desarrollar nuevas tecnologías y (iii) mayor concentración en el mercado de datos.

4.2. Las restricciones e ineficiencias económicas que podría generar el artículo 22 del RGPD en el mercado de datos

Tal como está redactado el artículo 22 del RGPD, pueden generarse ciertas ineficiencias económicas en el mercado de datos. Antes de analizar dichas ineficiencias una por una, resulta necesario explicar el concepto de mercado de datos y quienes interactúan en él.

El mercado de datos es el lugar en el que los agentes pueden comprar y vender datos, esencialmente a través de medios electrónicos. En Europa, se estima que para el año 2025 el valor del mercado de datos rondará entre los 199.510 y 334.210 millones de

⁹⁶ Comisión Europea, “*The European data market study update*”, 6 de julio 2020, recuperado el 13 de noviembre 2021 del sitio <https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update>.

euros⁹⁷, lo que demuestra la importancia que este mercado tendrá en un futuro no muy lejano. En este mercado, se intercambian datos y/o se prestan servicios relacionados con éstos.

Los agentes que interactúan en el mercado de datos son las empresas de datos y las empresas que son usuarias de datos. Las primeras son aquellas que ofrecen datos; es decir, que su actividad está vinculada con la producción y prestación de servicios de datos, como por ejemplo CA Technologies⁹⁸ (constituyen la parte oferente del mercado). Las segundas, son las que demandan esos datos para cumplir con su actividad económica principal (se posicionan desde el lado de la demanda del mercado).

Sentado lo anterior, pasaré a exponer sobre los posibles efectos restrictivos que el artículo bajo análisis podría generar.

4.2.A. Creación de una barrera legal a la entrada

Como adelanté, una de las ineficiencias económicas que puede causar la regulación prevista en el artículo 22 del RGPD es la creación de una barrera legal a la entrada al mercado de datos.

Las barreras a la entrada “...son los factores que impiden o dificultan la entrada de nuevos agentes económicos a un mercado. Estas barreras se pueden reflejar en diversos elementos de orden legal, tecnológico o económico, que afectan adversamente la probabilidad, oportunidad y suficiencia de la capacidad de entrada de nuevos participantes al mercado relevante, o de la capacidad de expansión de la escala de producción o comercialización de los participantes establecidos.”⁹⁹.

Dentro de los distintos tipos de barreras a la entrada, podemos encontrar las de carácter legal, que son aquellas regulaciones gubernamentales que restringen la cantidad de participantes del mercado a través de licencias, registros sanitarios, aranceles, etc.

⁹⁷ “Impacto de los datos abiertos”, recuperado el 13 de noviembre 2021 del sitio <https://data.europa.eu/es/impact-studies/open-data-impact>

⁹⁸ CA technologies, recuperado el 13 de noviembre de 2021 del sitio <https://www.capgemini.com/ar-es/partner/ca-technologies/>

⁹⁹ Diego Petrecolla, “Clases de defensa de la competencia. Módulo 3”. Diciembre 2019.

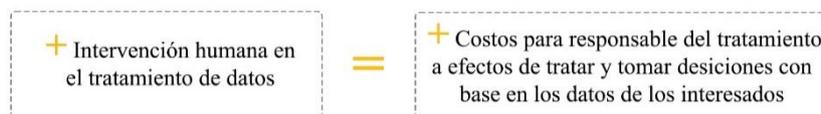
Entonces, vemos que esta barrera a la entrada tiene su origen en la regulación gubernamental y puede restringir el acceso al mercado a potenciales competidores; y en paralelo, también pueden causar efectos negativos en los consumidores, como precios más altos.

Así, estas barreras pueden generar que la prestación de servicios sea ineficiente y a su vez, causar daños a los consumidores en la medida que se les priva de un mayor bienestar. Y todo ello, en su conjunto, afecta la libre competencia en los mercados.

Sentado lo anterior, cabe señalar que el artículo 22 del RGPD podría causar una barrera legal a la entrada para los agentes interesados en participar del mercado relevante de datos europeo.

Al respecto, el apartado 3 del artículo 22 del RGPD contempla que *“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.”* (el subrayado me pertenece).

Así, con este inciso la autoridad regulatoria quiso proteger al interesado garantizándole la intervención humana en caso de errores u objeciones al tratamiento y toma de decisiones automatizada; sin embargo, terminó creando una barrera legal a la entrada, dado que incrementa los costos que los responsables del tratamientos deben afrontar para tratar y tomar decisiones con base en los datos de los interesados; ello, ponderando especialmente el inmenso volumen de información que los responsables del tratamiento tratan actualmente.



En este punto, resulta importante destacar que en atención a lo regulado por el apartado 3 del artículo 22 y de existir una impugnación de la decisión por parte del

interesado, los responsables del tratamiento deberán contratar mucha mano de obra adicional que se encargue de controlar los procesos de toma de decisiones. Reitero, teniendo en cuenta la gran cantidad y complejidad de los datos que se tratan actualmente.

Esto conlleva que los responsables del tratamiento deberán contratar una gran cantidad de trabajadores adicionales, para que los mismos supervisen manualmente el tratamiento de los datos personales de los interesados; y ello, indefectiblemente, hará el proceso de tratamiento de datos mucho más costoso para los responsables del mismo.

Como consecuencia de ello, vemos que la regulación prevista en el artículo bajo análisis puede impedir la entrada al mercado de datos a pequeñas y medianas empresas que no cuenten con los recursos económicos suficientes para cumplir con el RGPD (véase que, por ejemplo, muchas empresas debieron gastar millones de dólares para adaptarse y cumplir con esta norma¹⁰⁰).

Y ello a su vez, genera efectos anticompetitivos en dicho mercado de datos europeo.

En este punto, discrepo con el Grupo de Trabajo del Artículo 29, que expuso que el RGPD tiene efectos pro-competitivos para los responsables del tratamiento¹⁰¹; dado que no se consideró los efectos anticompetitivos mencionados con anterioridad, que dicha norma puede causar a dichos responsables.

En rigor, y ya pasados cuatro años de la sanción del RGPD, aún no se ha considerado dicha barrera legal a la entrada y los efectos anticompetitivos que ella genera para las empresas de datos y usuarias de datos.

¹⁰⁰ Chris Albert Denhart, “New European Union Data Law GDPR Impacts Are Felt By Largest Companies: Google, Facebook”, *Revista Forbes*, 25/5/2018, recuperado el 25 de diciembre de 2021 <https://www.forbes.com/sites/chrisdenhart/2018/05/25/new-european-union-data-law-gdpr-impacts-are-felt-by-largest-companies-google-facebook/#4b57c3414d36>.

¹⁰¹ Comisión Europea, Grupo de Trabajo del Artículo 29, “Directrices sobre el derecho a la portabilidad de datos del Reglamento 2016/679”, obtenido el día 25 de diciembre de 2021 del sitio web https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

Sentado lo expuesto, queda en evidencia una de las restricciones económicas que causa el artículo 22 del RGPD y que afecta la libre competencia entre los agentes del mercado relevante de datos europeo.

4.2.B. Desincentivos para innovar y desarrollar nuevas tecnologías

Otra ineficiencia económica que puede causar el artículo 22 del RGPD es el desincentivo a las empresas de datos a que desarrollen nuevas tecnologías/servicios y/o mejoren los ya existentes, lo que indirectamente afectaría el bienestar de los interesados dado que éstos se benefician de esas tecnologías y/o servicios.

Esta cuestión está íntimamente vinculada con el consentimiento del interesado y su ambigua regulación en el artículo bajo análisis.

En este punto, resulta importante señalar que *“El otorgamiento del consentimiento es de suma importancia, ya que es el mecanismo a través del cual se manifiesta la aceptación o rechazo del uso de los datos personales del individuo.”*¹⁰². Aquí, hago notar que el consentimiento del interesado es el fundamento legal¹⁰³ para que el responsable del tratamiento pueda efectuar la toma de decisiones automatizadas con base en la información recolectada de los usuarios y consumidores.

Si bien el artículo 4, inciso 11 del RGPD prevé 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”*, y el artículo 22 del RGPD dispone que **el consentimiento del interesado es necesario para que el responsable pueda realizar el tratamiento automatizado de toma de decisiones, la normativa aquí estudiada no establece si ese consentimiento es “general” o “particular”; es decir, no determina si para la toma de decisiones automatizadas con base en los datos**

¹⁰² Catalina Frigerio Dattwyler, *“Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho”*, Rev. chil. derecho tecnol. vol.7 no.2 Santiago dic. 2018, recuperado el 24 de diciembre de 2021 del sitio https://scielo.conicyt.cl/scielo.php?pid=S0719-5842018000200045&script=sci_arttext&tlng=p.

¹⁰³ Artículo 22, apartado. 2, inciso c del RGPD.

personales basta el consentimiento “inicial” del interesado; o bien, se necesita consentimiento para cada una de las veces que debe tomarse una decisión.

Si fuera un consentimiento general, el interesado debería hacer “futurología” y prever las eventuales decisiones futuras que se tomen con motivo de sus datos personales -ello, a los fines de poder objetar las mismas-. Esta circunstancia pone a los consumidores en una posición de desventaja en punto a su derecho de defensa. Por tanto, podría asumirse que los interesados no brindarían un consentimiento general en atención que no pueden predecir las futuras decisiones que se tomen con sus datos personales.

Por otra parte, si el consentimiento fuera particular, el responsable del tratamiento debería solicitar el consentimiento de los interesados cada vez que se tomara una decisión y esperar la aceptación de los mismos. Esta última situación podría generar altos costos de transacción debido a que insumiría mucho tiempo, sesgo de consentimiento o una intromisión a la vida privada de los interesados.

Y toda esta cuestión que involucra el consentimiento de los interesados podría impactar negativamente en los procesos de toma de decisiones automatizadas, ya que los mismos -que se basan en algoritmos autoeducados- podrían sufrir demoras para tomar decisiones con base a la información recolectada; retrasando el avance tecnológico de productos y servicios que se valen de esos datos personales.

Para ilustrar esta circunstancia en un caso concreto, vemos que en la industria de la construcción -más precisamente, en las casas inteligentes- es necesaria la recolección y tratamiento de datos de las personas que habitan la vivienda para desarrollar productos que hagan más eficiente el consumo de la energía (luz y gas) y del agua. Inclusive, esos datos resultan importantes para mejorar las condiciones de seguridad de la casa.

El sistema que utiliza big data analiza los patrones de comportamiento de múltiples individuos -teniendo en cuenta la cantidad de personas que habitan la casa- para hacer la vivienda más sustentable y segura; y ello permite a los proveedores de este bien mejorar la prestación del servicio. Lo que genera en paralelo que los proveedores compitan para ofrecer mejores productos que benefician no solo a las personas que

habitan la casa, sino también al medioambiente (en el caso del consumo eficiente de energía y recursos naturales).

Ahora bien, **si los responsables del tratamiento se ven obligados a requerir el consentimiento de cada persona que habita la vivienda, por cada vez que debe tomarse una decisión con base en sus datos personales, es evidente que el desarrollo de nuevas tecnologías para mejorar dicho bien tendrá retrasos.** Y esto es un desincentivo para innovar en estos productos.

Otro caso ilustrativo lo podemos encontrar en la industria automotriz (vehículos autónomos y semiautónomos). En un estudio realizado por el Massachusetts Institute of Technology¹⁰⁴ se sostuvo que los elementos de seguridad de los autos autónomos o semiautónomos necesitan en gran medida de la innovación de nuevas tecnologías -las que requieren necesariamente la recolección y el análisis de una serie de características del conductor al momento de manejar-.

Con relación a estos vehículos, resulta importante señalar que la recolección, tratamiento y análisis de la información no podría hacerse de manera manual, toda vez que la información recolectada involucra a 122 participantes y alrededor de 7.000.000.000 de imágenes corporales de los mismos que deben ser tratadas y analizadas.¹⁰⁵

Y dada la imposibilidad material de realizar el tratamiento de esos datos de manera manual, vemos que la regulación prevista en el apartado 3 del artículo 22 del RGPD perjudicaría el proceso de toma de decisiones automatizadas; no solo porque es materialmente imposible -una persona tardaría mucho tiempo en analizar todas esas imágenes-, sino que a su vez, demoraría el avance de la tecnología en materia de seguridad para estos vehículos.

¹⁰⁴ Lex Fridman, “MIT Autonomous Vehicle Technology Study: Large Scale Deep Learning Based analysis of Driver Behaviour and Interaction with Automation”, Massachusetts Institute of Technology, recuperado el 24 de diciembre de 2021 del sitio web <https://hcai.mit.edu/avt/> y del sitio web <https://lexfridman.com/avt/>.

¹⁰⁵ *Ibíd.*

Sentado todo lo anterior, surge a las claras que si se limita el uso de estas tecnologías, las empresas de datos -que proveen estos productos/servicios- tendrían obstáculos legales e innecesarios para competir entre sí a fin de desarrollar la mejor tecnología de tratamiento y análisis de datos personales. En paralelo, vemos que debido a la regulación prevista en el artículo estudiado, los agentes del mercado de datos tendrían un gran riesgo de violentar las disposiciones del RGPD -con las sanciones económicas que ello implica-; y en consecuencia, podrían ser muy pocas las empresas dispuestas a asumir ese riesgo.

En virtud de lo expuesto, vemos que el artículo 22 del RGPD puede generar desincentivos para que las empresas del mercado de datos innoven y desarrollen nuevas tecnologías en productos y/o servicios; y ello afecta indirectamente a los interesados, ya que, por ejemplo, si se limita o retrasa el desarrollo de nuevas tecnologías que mejoren la seguridad de los vehículos autónomos, se incrementa el riesgo de que los consumidores tengan accidentes.

4.2.C. Mayor concentración en el mercado de datos

Por su parte, el artículo 22 también puede causar una mayor concentración en el mercado de datos.

De manera preliminar, cabe señalar que según Diego Petrecolla *“Las operaciones de concentración económica pueden ser horizontales, verticales o de conglomerado. Esta clasificación obedece al nivel o segmento de mercado que se ve afectado por la operación.”*¹⁰⁶.

En este sentido, la concentraciones horizontales *“...involucran a competidores directos, actuales o potenciales, por lo que pueden eliminar la competencia directa entre dos empresas.”*¹⁰⁷ y las concentraciones verticales *“...involucran a empresas que operan en distintos niveles de la cadena de valor, y pueden producir dos principales efectos*

¹⁰⁶ Diego Petrecolla, *“Clases de defensa de la competencia. Módulo 3”*. Diciembre 2019.

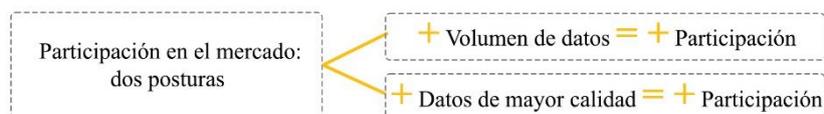
¹⁰⁷ *Ibíd.*

verticales nocivos: la obstaculización del acceso a insumos y la obstaculización del acceso a la clientela.”.

A su vez, los conglomerados “...involucran empresas que operan en diferentes mercados, aunque podrían estar estrechamente relacionados, por ejemplo, porque involucran los mismos clientes, por ello son en principio menos lesivas para el proceso de competencia.”¹⁰⁸.

Sentado ello, adelanto que como consecuencia de la regulación prevista en el artículo 22, **en el mercado de datos podría darse una concentración vertical debido a que una misma empresa podría situarse en distintas etapas de la cadena de valor y obstaculizar la obtención de datos de buena calidad a otros agentes.**

Al respecto, señalo que existen dos posturas en punto a la manera de medir la participación de las empresas en el mercado de datos. La primera, postula que contar con mayores volúmenes de datos conlleva tener una mayor participación en el mercado; y la segunda, sostiene que no importa la cantidad de datos que posean las empresas, sino la cualidad de esos datos¹⁰⁹. Bajo esta postura, la participación de una empresa en el mercado de datos estará determinada por la calidad de los datos, su finalidad, la calidad de la base de datos que tiene la organización y los algoritmos utilizados en el tratamiento de los datos.



En mi opinión, esta última es la visión más acertada para medir la participación de las empresas en el mercado de datos, dado que lo realmente importante es que los datos recolectados y tratados por las empresas sean buenos y utilizables para un fin determinado -por ejemplo, para la toma de una decisión-. Por el contrario y respecto de la postura de “*mayor volumen = mayor participación*”, advierto que existen muchos “datos basura”

¹⁰⁸ *Ibid.*

¹⁰⁹ Torsten Körber, “*Data, Platforms and Competition Law*”, obtenido el 25 de diciembre de 2021 del sitio web http://ec.europa.eu/competition/information/digitisation_2018/media_en.html.

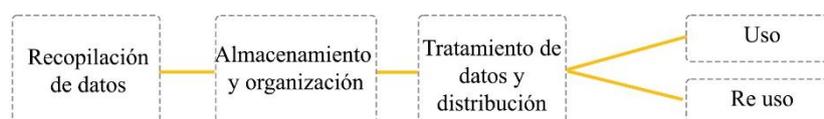
que podrían engrosar el volumen de datos tratados por cierta empresa, pero que en realidad no tienen ningún valor real porque no son utilizables para ningún fin. Es por ello, que a mi criterio, este último postulado no puede determinar realmente la participación de una empresa en el mercado de datos.

Siguiendo con el análisis de la concentración en el mercado de datos, cabe señalar que en atención a la regulación del RGPD, y en particular del artículo 22, las grandes empresas de datos podrían dejar de compartir entre sí los mismos. Ello, con motivo de los rigurosos recaudos exigidos a los responsables del tratamiento.

Así, las grandes empresas de datos como Google, Meta, Microsoft, Apple y/o IBM tendrán un mejor desarrollo de tecnologías de productos y/o servicios con base en datos personales, dado que tienen mayores recursos económicos y acceso a datos de mejor calidad, mientras que a las pequeñas y medianas empresas (start-ups) le será más difícil y costoso obtener estos “datos buenos” para innovar y mejorar sus tecnologías. Y ello, indirectamente, impactará negativamente en los consumidores dado que habrá un menor espectro de oferentes de bienes y servicios y un incremento en el precio de los servicios.

Entonces, y siguiendo la postura de “*mayores datos de mejor calidad = mayor participación en el mercado*”, las grandes empresas tendrían una mayor participación en el mercado de datos.

A la vez, **la concentración vertical podría ocurrir en el mercado de datos, toda vez que las grandes empresas podrían adquirir otras más pequeñas e instalarse en distintas etapas de la cadena de valor.** Estas etapas son, (i) la recopilación de datos; (ii) almacenamiento y organización; (iii) tratamiento de datos y distribución y, finalmente, (iv) su uso y re uso.



Por ejemplo, una empresa que cuenta con bases de datos (etapa de almacenamiento y organización) podría fusionarse a otra que preste servicios de

tratamiento y análisis de datos (etapa de tratamiento), incrementando así su participación en el mercado de datos y concentrando más el mismo.

Por lo tanto, **las empresa con mayores recursos y acceso a los datos de mejor calidad tenderán a acaparar y consolidarse en más de una etapa de la cadena de valor; y ello producirá una mayor concentración en el mercado bajo estudio (principalmente en la etapa de tratamiento de datos); máxime, si se tiene en cuenta que este mercado es proclive a concentrarse**¹¹⁰.

Al respecto, cabe señalar que si bien podría encontrarse una solución a esta situación con una reforma del régimen de control de integraciones, el Grupo de Consulta del Consumidor Europeo propone que existan mayores controles al cumplimiento del RGPD, omitiendo considerar que el propio reglamento es el que podría causar esa mayor concentración en un mercado que es propenso a ello.

En virtud de lo expuesto, remarco que si no se modifica o repiensa el artículo 22, podría generarse la situación anticompetitiva señalada; ello, en favor de las grandes empresas de datos y en perjuicio de los interesados.

¹¹⁰ 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*”, obtenido el día 26 de diciembre de 2021 del sitio web https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf.

5. EXTERNALIDADES NEGATIVAS EN LOS PROCESOS AUTOMATIZADOS DE TOMA DE DECISIONES: LA DISCRIMINACIÓN

Los procesos automatizados de toma de decisiones, en ciertos casos, generan externalidades negativas que afectan los derechos y libertades de las personas cuyos datos se tratan.

En esta línea, cabe señalar que muchas veces la información que se incorpora a los algoritmos de estos procesos automatizados contiene sesgos y/o prejuicios que causan resultados discriminatorios; o bien, son utilizados para manipular la voluntad de los usuarios y consumidores.

Así, uno de los argumentos que se esgrime para fundar la restricción y/o limitación del uso de los procesos automatizados de toma de decisiones, es precisamente la discriminación. Sin embargo, y como veremos más adelante, la discriminación no tiene su causa intrínseca en dichos algoritmos/procesos, sino que su origen proviene de factores exógenos (el input/información que los programadores incorporan en los algoritmos), no siendo la limitación de estos procesos automatizados la mejor solución al problema.

5.1. La discriminación como fundamento para restringir los procesos automatizados de toma de decisiones

Como señalé anteriormente, la discriminación¹¹¹ es el principal argumento que se utiliza para fundar la limitación de los procesos automatizados de toma de decisiones; restricción que se materializó en el artículo 22.

En este sentido, cabe señalar que si bien es cierto que muchas veces los procesos automatizados de toma de decisiones pueden causar externalidades negativas¹¹² en los usuarios y consumidores, ello no implica que deba restringirse su uso y/o aplicación como lo dispone la norma bajo estudio, toda vez que pueden adoptarse alternativas para

¹¹¹ Acción de tratar a una persona física o jurídica o a un grupo de personas de manera menos favorable que a otras personas que se encuentran en una situación comparable.

¹¹² Que son aquellas consecuencias de cierta actividad que afectan desfavorablemente a terceros ajenos a la misma. Por ejemplo, fumar en un espacio cerrado, afecta negativamente a quienes se encuentran también en dicho espacio y no fuman.

erradicar esa discriminación y para que los procesos de toma de decisiones actúen libremente, sin ninguna restricción.

Al respecto, el Grupo de Trabajo del artículo 29 del RGPD sostuvo que la aplicación de los procesos automatizados de toma de decisiones y la elaboración de perfiles podría llevar a que se realicen predicciones erróneas sobre las preferencias de los interesados y ello, indirectamente, podría afectar la libre voluntad de los mismos¹¹³. Por ejemplo, porque a un interesado se le podría sugerir/ofrecer un producto o servicio en base a su raza o creencia, sin siquiera tener un conocimiento certero de que si a esa persona le interesa –o no- ese producto o servicio.

En términos simples, se puede ofrecer un producto o servicio en base a un perfil -creado por algoritmos que han sido programados con algún sesgo- que muchas veces puede no coincidir con las preferencias del interesado.

Ahora bien, adelanto que esa discriminación podría ser eliminada si quienes utilizan big data y programas con machine learning para dichos procesos fueran más transparentes e invirtieran en investigaciones para corregir los errores que actualmente tienen los mismos. Reitero, estas inconsistencias no son creadas por los procesos en sí mismos, sino por la información sesgada que se incorpora a los algoritmos.

Así, vemos que los procesos automatizados de toma de decisiones y los algoritmos que los conforman están diseñados por personas que, voluntaria o involuntariamente, incorporan en los algoritmos los prejuicios y estereotipos que tienen respecto de ciertos grupos sociales. Aquí, resulta importante señalar que uno de los motivos de la incorporación de estos inputs sesgados es la conformación de equipos de programadores de sistemas, que en general son hombres blancos heterosexuales que provienen de sectores sociales acomodados y que en ciertos casos, han estado a favor de

¹¹³ Comisión Europea, Grupo de Trabajo del artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”, obtenidas el día 1 de enero de 2022 del sitio web https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

posturas que exponen la idea de que las personas pertenecientes a ciertos grupos sociales -históricamente discriminados- son inferiores¹¹⁴.

Cabe aclarar que los algoritmos no son totalmente autónomos, sino que toda decisión automática basada en algoritmos necesita de un humano para determinar la decisión deseada bajo cierta condición (dado un input “A” resultará un output “B”)¹¹⁵.

Entonces, habida cuenta que los algoritmos procesan una suerte de “realidad social” que es creada sobre la base de preconceptos que discriminan a personas que forman parte de grupos sociales históricamente segregados; la consecuencia de ello es que los procesos automatizados de toma de decisiones incorporan y replican esa estructura discriminatoria¹¹⁶.

Sentado ello, a continuación, se expondrán algunos casos prácticos en los cuales existió discriminación de los procesos automatizados debido a los inputs sesgados de los programadores; para luego pasar a explicar las alternativas que podrían solucionar este problema, sin la necesidad de restringir estos procesos.

5.2. Casos de discriminación de los procesos automatizados de toma de decisiones

Muchos han sido los casos en que como consecuencia de los sesgos incorporados a los algoritmos que conforman los procesos automatizados de toma de decisiones, se ha discriminado a grupos de personas históricamente segregados.

Veamos:

➤ **El caso Amazon:** En el año 2014, Amazon creó un programa basado en inteligencia artificial para optimizar el proceso interno de revisión de currículums, a los

¹¹⁴ Alba Soriano Arnanz, “Decisiones Automatizadas: Problemas Y Soluciones Jurídicas. Más Allá De La Protección De Datos” Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales Vol. 3 | 2021 pág. 85-127. Madrid, 202.

¹¹⁵ Ignacio Cofone, “Algorithmic Discrimination is an information problema”, Hasting Law Journal, pág. 1400.

¹¹⁶ *Ibíd.*

finés de sumar talento a la empresa¹¹⁷. Este programa otorgaba a los candidatos un puntaje entre una y cinco estrellas -sistema similar al que tienen los compradores de Amazon para evaluar a los vendedores-.

Ahora bien, en el año 2015, la compañía descubrió que dicho sistema no evaluaba de igual manera a candidatos y candidatas para el puesto de desarrollador/a de sistemas y otros puestos técnicos. Es decir, Amazon advirtió que dicho sistema de selección discriminaba a las postulantes mujeres con motivo de su género.¹¹⁸

Y ello fue así debido a que los algoritmos creados por los programadores de Amazon fueron “entrenados” para analizar candidatos comparando patrones de aquellos curriculums que la compañía había recibido para puestos similares a lo largo de diez años, curriculums que provenían en su mayoría de hombres, debido a la predominancia de este género en la industria tecnológica algunos años atrás¹¹⁹.

Así, el sistema creado por el algoritmo creado por los programadores de Amazon se enseñaba así mismo que los candidatos hombres eran preferibles respecto de las mujeres. En consecuencia. Toda esta situación llevó a que Amazon diera de baja dicho programa para captar talento para su empresa.

➤ **El caso Word2Vec:** En el año 2013, Tomas Mikolov diseñó un software para el procesamiento del lenguaje natural. A través de un algoritmo creado a tal efecto, Word2Vec utiliza un modelo de red neuronal para aprender asociaciones de palabras de un texto¹²⁰. Este software asocia e incorpora palabras en el cuerpo de un texto. En este contexto, Bolukbasi demostró que en este programa la palabra hombre estaba asociada con la de “programador de computadoras”, mientras que la palabra mujer con la de “ama de casa”, de modo que la discriminación provenía de la información que los

¹¹⁷ Jeffrey Dastin, “Amazon scraps secret AI recruiting tool that showed bias against women”, 10/10/2018, Reuters, obtenido el 2 de enero de 2022 del sitio web <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>

¹¹⁸ Ibid.

¹¹⁹ Ibid.

¹²⁰ Dhruvil Karani, “Introduction to Word Embedding and Word2Vec” 1/10/2018, Towards Data Science, obtenido el 2 de enero de 2022 del sitio web <https://towardsdatascience.com/introduction-to-word-embedding-and-word2vec-652d0c2060fa>.

programadores de este programa incorporaban a los algoritmos encargados de llevar adelante el software¹²¹.

Peor aún es el hecho de que el sesgo y/o prejuicio incorporado en este programa se había propagado mediante cualquier otro sistema o programa que utilizara como base el mismo.

En este caso, la discriminación hacía la mujer, también provendría de los programadores que crearon y diseñaron el programa, quienes asociaban la palabra hombre a su profesión trabajo.

➤ **El caso COMPAS (Correctional Offender Management Profiling for Alternative Sanctions):** Hace unos años atrás, Northpointe (ahora conocido como Equivant¹²²) creó un algoritmo llamado COMPAS que permitía medir la posibilidad de reincidencia de delitos de una persona. El algoritmo fue diseñado para predecir la posibilidad de que una persona -con antecedentes penales- reincidiera en el plazo de dos años. Así, COMPAS era utilizado para predecir la comisión de futuros crímenes por parte de personas que habían sido arrestadas con anterioridad¹²³.

Ahora bien, ProPublica acusó a COMPAS de tener sesgos raciales en sus resultados, teniendo dos veces más de falsos positivos respecto de acusados de piel negra que de acusados de piel blanca y más falsos negativos en acusados con piel blanca que con acusados de piel negra¹²⁴.

En términos simples, el algoritmo erróneamente interpretaba que había un mayor riesgo de reincidencia de los acusados de piel negra que de aquellos de piel blanca. Desde

¹²¹ Tolga Bolukbasi, Kai-Wei Chang, James Y Zou, Venkatesh Saligrama, and Adam T Kalai. Man is to computer programmer as woman is to homemaker? debiasing word embeddings. In D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, editors, *Advances in Neural Information Processing Systems 29*, pages 4349-4357. Curran Associates, Inc., 2016. Obtenido el 2 de enero de 2022 del sitio web papers.nips.cc/paper/6228-man-is-to-computer-programmer-as-woman-is-to-homemaker-debiasing-word-embeddings.pdf.

¹²² Equivant (<https://www.equivant.com/about-us/>).

¹²³ Ignacio Cofone, “*Algorithmic Discrimination is an information problem*”, *Hasting Law Journal*, pág. 1396.

¹²⁴ *Ibid.*

entonces, decenas de artículos han criticado el uso de este algoritmo debido al claro sesgo discriminatorio incorporado por quienes lo diseñaron.

Este es otro claro ejemplo de que la discriminación ha sido incorporada con la información que crea y enseña al algoritmo a realizar los procesos automatizados.

Con los casos ilustrados anteriormente, vemos que la discriminación no resulta ser una creación propia de los procesos automatizados de toma de decisiones, sino que la misma proviene de la información sesgada e incorporada a los algoritmos que componen estos procesos.

En este sentido, y si bien la discriminación causada a raíz del diseño sesgado de los algoritmos es un argumento empleado para limitar la utilización de los procesos automatizados de toma de decisiones; lo cierto es que existen ciertas medidas alternativas para erradicar la discriminación y no intervenir en estos procesos automatizados; lo que expondré seguidamente.

5.3. Medidas alternativas para erradicar la discriminación y así, aprovechar las ventajas de los procesos automatizados de toma de decisiones

5.3.A. Existen distintas medidas/reglas para reducir y/o erradicar la discriminación en los algoritmos, y consecuentemente, en los procesos automatizados de toma de decisiones.

En economía, la discriminación es definida como el problema de no contar con suficiente información de los demás¹²⁵. Teniendo en cuenta esto, una persona puede juzgar a otra sin contar con información suficiente, lo que causaría una opinión falsa/incompleta¹²⁶. Así, y si consideramos que la discriminación es un problema de no contar con información suficiente sobre los demás, vemos que tal discriminación sería de naturaleza estadística en lugar de estar basada en sesgos psicológicos o prejuicios.

¹²⁵ Lior Jacob Strahilevitz, "Privacy Versus Antidiscrimination", 75 U. Chi. Rev. 363,364.

¹²⁶ Ignacio Cofone, "Algorithmic Discrimination is an information problema", Hasting Law Journal, pág. 1408.

Entonces, si entendemos que la discriminación está vinculada con cuestiones cuantitativas (contar con más o menos información sobre las personas) y no con sesgos psicológicos, crear y dar más acceso de nuestra información personal reduciría la discriminación; ello, debido a que los algoritmos podrían contar con información completa para tratar y tomar decisiones.

En otras palabras, crear un espectro de información completa respecto los interesados reduciría la discriminación, mientras que aumentar la regulación sobre la privacidad la empeoraría -dado que esto crea información incompleta-.

En este sentido, Strahilevitz ha afirmado que *“al aumentar la disponibilidad de información de los individuos podemos reducir la dependencia de los algoritmos en la información sobre ciertos grupos sociales”* (traducción propia)¹²⁷.

Desde este punto de vista económico, **los interesados deberían tolerar la discriminación “estadística” dado que la única manera de erradicar la discriminación es brindar mayor información a los algoritmos.**

5.3.B. En otro orden, programar el algoritmo para que bloquee cierta información individual de los interesados (en el proceso de toma de decisiones automatizado), sería otra solución al problema de la discriminación.

Al respecto, reitero que el sesgo algorítmico precede al algoritmo, porque el sesgo existe en el dato/información con que es alimentado el algoritmo. Los datos utilizados para crear un sistema de machine learning determinan cómo el sistema interpreta el área sobre el cual opera para hacer predicciones y tomar decisiones. Entonces, toda vez que el sesgo algorítmico precede al algoritmo, son las reglas de antidiscriminación de la información aquellas que resultan más útiles para resolver el problema de la discriminación.

A diferencia de las personas humanas, los algoritmos pueden bloquear determinados puntos de información en el proceso de toma de decisiones. Mientras que sería difícil instruir a una persona a que sea indiferente ante un hecho visible, es más

¹²⁷ Lior Jacob Strahilevitz, *“Privacy Versus Antidiscrimination”*, 75 U. Chi. Rev. 364.

probable -aunque no simple- programar un algoritmo para que si lo sea. Es decir que se puede programar un algoritmo para cada variable. Por ejemplo, comparar el salario de contratación cuando se incluye la información de la religión de los alicantes de cuando se bloquea esa información.

Así, en los procesos de toma de decisiones automáticas es posible recopilar determinada información e instruir a los algoritmos a que ignoren ciertos hechos o puntos de esa información mientras hacen la predicción y toman la decisión.

Por tanto, vemos que si se enseña al algoritmo a bloquear/ignorar la información sesgada que incorporan los programadores, se reduciría la discriminación en los procesos de toma de decisiones.

3.5.C. Por su parte, la Agencia de Derechos Fundamentales de la Unión Europea también ha propuesto medidas alternativas para aprovechar los beneficios de los procesos automatizados de toma de decisiones y erradicar la discriminación de los mismos. Estas propuestas consisten en crear sistemas más transparentes, realizar evaluaciones de impacto, corroborar la calidad de la información y asegurar que los algoritmos puedan ser explicados y comprendidos¹²⁸.

Así, la primera propuesta pretende fomentar una mayor libertad en las decisiones tomadas por los interesados y permite que los mismos estén interiorizados con la manera mediante la cual funcionan los procesos automatizados de toma de decisiones.

A su vez, las evaluaciones de impacto permitirían identificar cuáles son los potenciales sesgos introducidos en los algoritmos e implica una evaluación sobre diferentes clases de discriminación como aquellas basadas en el género, raza, edad, religión, etc.

También es necesario corroborar la calidad de los datos recopilados y utilizados en el proceso de toma de decisión para verificar su calidad y, finalmente, resulta fundamental que los interesados entiendan cómo funcionan los algoritmos.

¹²⁸ Agencia de los Derechos Fundamentales de la Unión Europea, “*Big Data: Discrimination in Data Supported Decision Making*”, obtenido el 8 de enero de 2022 del sitio web https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf.

3.5.D. En virtud de todo lo expuesto, vemos que los procesos automatizados de toma de decisiones podrían adoptar medidas alternativas para eliminar una de sus externalidades negativas (la discriminación).

En este capítulo, quería dejar sentado que existen medidas para paliar los posibles efectos negativos que estos procesos pueden causar a los interesados; no siendo las regulaciones normativas el mejor remedio para estas cuestiones.

Como se puede ver en el artículo 22 del RGPD, la limitación que dicha norma causa sobre los procesos automatizados bajo estudio es evidente, y, a mi criterio, hay que apelar a la creatividad para encontrar soluciones novedosas que nos permitan saltar los obstáculos o inconvenientes que la tecnología –o en este caso, los programadores- puede generar actualmente.

Es por ello que remarco -una vez más- que dicho artículo debería ser modificado para otorgar mayores libertades a los responsables del tratamiento, a los efectos de que éstos puedan desarrollar nuevas tecnologías y competir libremente en el mercado de datos; mejorando con ello sus productos/servicios y el bienestar agregado de los interesados.

En este sentido, y a continuación, desarrollaré las conclusiones de cada uno de los puntos centrales analizados en el presente trabajo y de la hipótesis planteada.

6. CONCLUSIONES

Como corolario de todos los puntos analizados a lo largo de esta tesis, en el presente capítulo desarrollaré las conclusiones de las cuestiones centrales del trabajo y en particular, de la hipótesis de investigación planteada.

6.1. Las restricciones e ineficiencias económicas creadas en el mercado de datos como consecuencia de la regulación prevista en el artículo 22 del RGPD

Llegada la conclusión, cabe señalar que a lo largo del presente trabajo expuse las razones por las cuales entiendo que la regulación prevista en el artículo 22 del RGPD puede ocasionar ciertas restricciones e ineficiencias económicas en el mercado de datos y la libre competencia económica.

El artículo 22 puede: (i) crear una barrera legal a la entrada; (ii) ser un desincentivo para la innovación tecnológica; y (iii) causar una mayor concentración en el mercado de datos. Y en paralelo, expliqué que el principal argumento utilizado para justificar esta regulación se basa en la discriminación que realizan los procesos automatizados de toma de decisiones al ser aplicados en alguna industria y/o campo de estudio en particular.

Así, y en punto a las ineficiencias mencionadas en el párrafo anterior, vemos que el artículo 22 puede crear una **barrera legal a la entrada en el mercado de datos europeo**, toda vez que no permite que todas las decisiones automatizadas se basen únicamente en el tratamiento de datos automatizados. Al respecto, es el apartado 3 del artículo 22 el que limitaría el trabajo de los procesos automatizados y crearía un aumento en los costos para los responsables y/o encargados del tratamiento, quienes deberían contratar más personal a fin de controlar, tratar y tomar decisiones con base en los datos de los interesados.

Esto, considerando que hoy en día los volúmenes de información que tratan los responsables y/o encargados del tratamiento son enormes.

Por lo tanto, podríamos concluir respecto a este punto, que la regulación prevista en el apartado en cuestión haría que se restrinja la entrada de aquellas pequeñas y medianas empresas que no cuentan con los recursos suficientes para contratar personal adicional a fin de controlar la toma de decisiones de los procesos automatizados; es decir, se restringiría la entrada de estas empresas (start-ups) al mercado de datos europeo.

En adición, **esta norma también puede desincentivar la innovación tecnológica**. Como vimos en el capítulo 4, el consentimiento del interesado y su ambigua regulación en el artículo bajo análisis, generan dudas sobre la legalidad del tratamiento y toma de decisión en distintas industrias y campos de investigación. Esto podría desincentivar su desarrollo, lo que indirectamente causaría un retraso en el surgimiento de nuevas tecnologías que beneficien a los consumidores de ciertos productos y servicios.

Entonces, si el consentimiento no se encuentra bien definido y/o se halla limitado en esta regulación, tanto las empresas de datos como las empresas usuarias de datos se verían limitadas a competir unas con otras para brindar una mayor calidad en sus servicios.

Por su parte, también podríamos considerar que la regulación contemplada en el artículo 22 de la RGPD **podría ser la causa de una mayor concentración vertical en el mercado de datos**. En atención a las sanciones previstas en el RGPD y las graves consecuencias que ellas representan para los sujetos incumplidores, muchas compañías se verían inducidas a tercerizar el servicio de tratamiento y análisis de datos personales en grandes empresas que cuentan con la capacidad estructural y financiera para obtener datos de calidad; y serían estas grandes empresas las que al final del día tenderían a acaparar más mercado para ellas y concentrar el mismo.

Es por ello que concluyo, al respecto, que este artículo también puede generar mayor concentración en este mercado de datos.

Finalmente, y con relación a la justificación de esta norma, **cabe recordar que tampoco es sólido el argumento de la discriminación para fundar la regulación prevista en el artículo 22**. Ello, toda vez que la discriminación no es un problema intrínseco del tratamiento de los datos, sino que proviene del input (elemento externo) que los programadores incorporan en los algoritmos.

Así, este problema se podría solucionar con las alternativas planteadas en el capítulo 5 y no con la limitación/restricción los procesos automatizados de toma de decisiones.

6.2. Conclusión final

En virtud de todo lo expuesto a lo largo del presente trabajo, vemos que la regulación del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos puede crear restricciones e ineficiencias económicas en el mercado de datos; ello, en línea con lo planteado en la hipótesis.

Si bien considero que la regulación de este derecho ha puede significar un gran avance en materia de privacidad, no es menos importante el hecho de que, en su intento de proteger a los consumidores, este artículo afectaría valores económicos fundamentales como la eficiencia, la competencia y/o el bienestar de los interesados y, como consecuencia de ello, afectaría indirecta y negativamente a éstos.

En este sentido, y en mi opinión, entiendo que debería modificarse la redacción del artículo 22, y con ello cambiar y/o suprimir ciertos apartados del mismo, que son en definitiva los que ocasionarían las ineficiencias económicas señaladas. Por ejemplo, en el apartado 3 del artículo 22, eliminaría la frase “...*como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.*”; ello, a fin de evitar el problema del incremento de costos en mano de obra y la consecuente creación de una barrera legal a la entrada para los agentes interesados en participar del mercado relevante de datos europeo.

Más allá de ello, en este trabajo he analizado diferentes aspectos del artículo bajo análisis, y creo que con ello se ha evidenciado los potenciales efectos negativos que esta norma también podría generar en la innovación de nuevos productos y servicios; como así también los efectos anticompetitivos que se causarían en el mercado de datos.

Sumado a lo anterior, también hay que tener en cuenta que los sistemas de tratamiento automatizado de datos aún están en pleno desarrollo; razón por la cual,

debería dársele más libertad a los responsables y/o encargados del tratamiento para que puedan mejorar la calidad de los mismos.

Han pasado solo cuatro años de la entrada en vigencia del RGPD y aún hay un largo camino por recorrer en materia de privacidad. Solo el tiempo y los casos que se presenten con relación al artículo 22 determinarán si el mismo protege debidamente a los consumidores; o bien, los perjudica al restringir la eficiencia, innovación y libre competencia económica en el mercado de datos europeo.

7. BIBLIOGRAFÍA

- Matt Burges, “*What is GDPR? The summary guide to GDPR compliance in the UK*”. No hay fecha. www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.
- Julie Brill, “*GDPR’s first anniversary: A year of progress in privacy protection*”. 2019.
- Samuel Noah Kramer, “La historia empieza en Sumer”, Ediciones Orbis SA, 1985, pág. 17-21.
- José Antonio Castillo Romero, “*Big Data. IFCTI28PO*”, Ed. Ic, 2018, pág. 7.
- Inés Lujan, “*La imprenta y su impacto en la historia*”, Universidad de Valencia, No hay fecha. <https://www.uv.es/uvweb/master-historia-formacion-mundo-occidental/es/blog/invencion-imprenta-impacto-historia-1285960141137/GasetaRecerca.html?id=1285961209839>.
- Frank da Cruz, “*Herman Hollerith*”, Columbia University, 2021, recuperado el 1 de abril de 2021 de <http://www.columbia.edu/cu/computinghistory/hollerith.html>.
- José Antonio Castillo Romero, “*Big Data. IFCTI28PO*”, Ed. Ic, 2018, pág. 7.
- Ranjit Kaur, Parveen Kumar, Raminder Pal Singh, “*A Journey of Digital Storage from Punch Cards to Cloud*”, IOSR Journal of Engineering (IOSRJEN), 2014, pág. 37.
- Konrad Zuse, “*The computer – My life*”, Ed. Springer Verlag, 1984, 1986, 1990, 1993, pág. 32-35.
- Crypto Museum, “*Colossus of the Digital Computer*”. No hay fecha. <https://www.cryptomuseum.com/crypto/colossus/index.htm#:~:text=Birth%20of%20the%20digital%20computer&text=It%20was%20used%20to%20break,before%20the%20American%20ENIAC%20computer>.

- Institució Alfons el Magnànim-Centre Valencià d'Estudis i d'Investigació "El primer ordenador del mundo cumple años". No hay fecha. <http://www.conec.es/historia/%E2%80%A8el-primer-ordenador-del-mon-compleix-anys/>.
- Engineering and Technology, "ENIAC". No hay fecha <https://ethw.org/ENIAC>.
- J. G. Charney – A. Eliassen, "A Numerical Method for Predicting the Perturbations of the Middle Latitude Westerlies", Tellus, 1:2, 38-54, DOI: 10.3402/tellusa.v1i2.8500.
- Peter Lynch, "The origins of computer weather prediction and climate modeling", Journal of Computational Physics, 2008, pág. 3431-3444.
- Graham Singer, "History of the Microprocessor and the Personal Computer, Part 2". No hay fecha. <https://www.techspot.com/article/884-history-of-the-personal-computer-part-2/>.
- World Wide Web Foundation, "History of the Web". No tiene fecha, <https://webfoundation.org/about/vision/hisoty-of-the-web/>.
- Silvia Lago Martínez, "Ciberespacio y resistencias. Exploración en la cultura digital", Hekht libros, 2012, pág. 57.
- Sergio Luján Mora, "Programación de aplicaciones web: historia, principios básicos y clientes web", Ed. Club Universitario, 2002, pág. 27-28.
- I. Kuster – A. Hernandez, "De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención de uso de las redes sociales en la web semántica", Universia Business Review, 2013, pág. 111-119.
- S. Warren – L. Brandeis, "The right to privacy", Harvard Law Review, 193, 15/12/1890.
- Ernesto Clímaco Valiente, "Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento", Universidad III Carlos de Madrid, 2012, pág. 16-17.
- Court of Appeals of Kentucky, "Brents vs. Morgan", 15/11/1927, <https://www.casemine.com/judgement/us/5914a723add7b049346e74a1>.

- Supreme Court of The Unites States, “*Olmstead et al. v. United States*”, 4/6/1965, <https://www.law.cornell.edu/supremecourt/text/277/438>.
- Supreme Court of The Unites States, “*Estelle T. Griswold et al. Appellants, v. State of Connecticut*”, 7/6/1965, <https://www.law.cornell.edu/supremecourt/text/381/479>.
- William Prosser, “*Privacy*”, California Law Review v. 98, 1960.
- Edward Bloustein, “*Privacy, Tort Law, and Constitution: Is Warren and Brandeis’ tort petty and unconstitutional as well?*”, Texas Law Review, v. 46, 1968.
- Tribunal Constitucional Alemán, 15/12/1983, BVerfGE 65,1, <https://revistasonline.inap.es/index.php/DA/article/view/4687/474>.
- 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).
- Consejo de Europa, “*art. 8 de la Convención Europea de Derechos Humanos*” 3/9/1950, <https://www.derechoshumanos.net/Convenio-Europeo-de-Derechos-Humanos-CEDH/#a8>.
- Parlamento Federal Alemán, “*Ley Federal de Protección de Datos*”, 27/1/1977, https://www.bgbl.de/xaver/bgbl/media/DD5B0A8907DA04DC249329E46ACA760B/bgbl177i0201_39307.pdf.
- Jos Dumortier, “*Aplicación de la Directiva de Protección de Datos en Bélgica*”, Universidad Pontificia Comillas, Madrid, 1996 - 1997, pág. 51/74.
- Elisenda Bru Cuadrada, “*La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad*”, septiembre de 2007, <https://www.redalyc.org/pdf/788/78812861008.pdf>.
- European Data Protection Supervisor, “*The History of the General Data Protection Regulation*”, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

- Alejandra M. Gils Carbó, “*Régimen Legal de la Bases de Datos y Habeas Data*” LL, Buenos Aires, 2001, pág. 47.
- Pablo A. Palazzi, “*Protección de datos personales: Doctrina y Jurisprudencia*”, CETyS, Tomo 1, pág. 28.
- Julie Brill, “*GDPR’s first anniversary: A year of progress in privacy protection*”. No hay fecha. <https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/>.
- Forbes Technologies Council “*15 Unexpected Consequences Of GDPR – Forbes*” No hay fecha. <https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=5bc3bbaa94ad>.
- 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 , Vol 8, No 1, 2017), pág. 8.
- Comité Europeo de Protección de Datos, “*Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3)*” 12/11/2019, pág. 5, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_es.pdf.
- Sonia Vásquez y Javier de Miguel, “*Nuevo Régimen Sancionador De Protección De Datos*”, Revista Economist & Jurist. No hay fecha. <https://ecija.com/wp-content/uploads/2017/06/Sanciones-RGPD.pdf>.
- Information Commissioner’s Office, “*What is automated decision making including profiling?*”. 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>.
- Comisión Europea, Grupo de Trabajo del Artículo 29, “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*”. No hay fecha. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

- Mendoza, I. y Bygrave, L.A. “*The right not to be subject to automated decision based on profiling. In EU Internet Law: Regulation and Enforcement*” pág. 77-79.
- Brkan. M. “*Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond*”, SSRN. No hay fecha. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901.
- BCRA y CAF. Encuesta de medición de capacidades financieras en Argentina, 2017.
- Roger Lanctot, “*Accelerating the Future: The Economic Impact of the Emerging Passenger Economy*”, Strategy Analytics, Intel, pág- 5. No hay fecha. 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
- Lex Fridman, Daniel E. Brown, Michael Glazer, William Angell, Spencer Dodd, Benedikt Jenik, Jack Terwilliger, Aleksandr Patsekina, 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. No hay fecha. <https://hcai.mit.edu/avt/>.
- Chelsey Colbert, “*Privacy Under the Hood: Towards an International Data Privacy Framework for Autonomous Vehicles*”, Universidad de Stanford. No hay fecha. <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>
- Sandeep Kumar and Mohammed Abdul Qadeer, “*Application of AI in Home Automation*”, IACSIT International Journal of Engineering and Technology, Vol. 4, No. 6, Diciembre 2012.

- Julia Belluz, “3 ways AI is already changing medicine”. No hay fecha. <https://www.vox.com/science-and-health/2019/3/15/18264314/ai-artificial-intelligence-deep-medicine-health-care>.
- Guido Stein, “La inteligencia artificial en la selección de personas”. No hay fecha. <https://www.harvard-deusto.com/la-inteligencia-artificial-en-la-seleccion-de-personas>.
- 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”, pág. 11, 16 de mayo de 2018. https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf
- Comisión Europea, “The European data market study update”, 6 de julio 2020. <https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-update>.
- “Impacto de los datos abiertos”. No hay fecha. <https://data.europa.eu/es/impact-studies/open-data-impact>.
- Chris Albert Denhart, “New European Union Data Law GDPR Impacts Are Felt By Largest Companies: Google, Facebook”, Revista Forbes, 25/5/2018.
- Comisión Europea, Grupo de Trabajo del Artículo 29, “Directrices sobre el derecho a la portabilidad de datos del Reglamento 2016/679”. No hay fecha. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
- Catalina Frigerio Dattwyler, “Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho”, Rev. chil. derecho tecnol. vol.7 no.2 Santiago, dic. 2018, https://scielo.conicyt.cl/scielo.php?pid=S0719-5842018000200045&script=sci_arttext&tlng=p.
- Lex Fridman, “MIT Autonomous Vehicle Technology Study: Large Scale Deep Learning Based analysis of Driver Behaviour and Interaction with

- Automation*”, Massachusetts Institute of Technology. No hay fecha.
<https://lexfridman.com/avt/>.
- Torsten Körber, “*Data, Platforms and Competition Law*”. No hay fecha.
http://ec.europa.eu/competition/information/digitisation_2018/media_en.html.
 - 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*”. No hay fecha. https://ec.europa.eu/info/sites/info/files/eccg-recommendation-on-ai_may2018_en.pdf.
 - Alba Soriano Arnanz, “*Decisiones Automatizadas: Problemas Y Soluciones Jurídicas. Más Allá De La Protección De Datos*” Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales Vol. 3 | 2021 pág. 85-127. Madrid, 202.
 - Ignacio Cofone, “*Algorithmic Discrimination is an information problema*”, Hasting Law Jornal, pág. 1400.
 - Jeffrey Dastin, “*Amazon scraps secret AI recruiting tool that showed bias against women*”, 10/10/2018, Reuters. No hay fecha.
<https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G>
 - Dhruvil Karani, “*Introduction to Word Embedding and Word2Vec*” 1/10/2018, Towards Data Science. No hay fecha.
<https://towardsdatascience.com/introduction-to-word-embedding-and-word2vec-652d0c2060fa>.
 - Tolga Bolukbasi, Kai-Wei Chang, James Y Zou, Venkatesh Saligrama, and Adam T Kalai. Man is to computer programmer as woman is to homemaker? debiasing word embeddings. In D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, editors, Advances in Neural Information Processing Systems 29, pages 4349{4357. Curran Associates, Inc., 2016
 - Ignacio Cofone, “*Algorithmic Discrimination is an information problema*”, Hasting Law Jornal, pág. 1396.

- Lior Jacob Strahilevitz, "*Privacy Versus Antidiscrimination*", 75 U. Chi. Rev. 363,364.
- Ignacio Cofone, "*Algorithmic Discrimination is an information problema*", Hasting Law Jornal, pág. 1408.
- Lior Jacob Strahilevitz, "*Privacy Versus Antidiscrimination*", 75 U. Chi. Rev. 364.
- Agencia de los Derechos Fundamentales de la Unión Europea, "*Big Data: Discrimination in Data Supported Decision Making*", obtenido el 8/1/2022 del sitio web https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf.