IUS REVISTA DEL INSTITUTO DE CIENCIAS JURÍDICAS DE PUEBLA, MÉXICO. E-ISSN 1870-2147. NUEVA ÉPOCA VOL. 15, No. 48. JULIO - DICIEMBRE DE 2021. PP209-242

El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición?*

The Data Subject, Weak Party in the Rise of Artificial Intelligence. How to Strengthen his Position?

María Mercedes Albornoz**

RESUMEN

Un área en la que se manifiesta la tensión entre la innovación tecnológica que la Inteligencia Artificial (IA) supone y la protección de datos personales es la del consentimiento del titular. En efecto, la IA desafía el alcance y la validez del consentimiento. Se considera, sin embargo, que continúa siendo una opción jurídicamente relevante para habilitar el tratamiento lícito de datos personales por parte del responsable. Por eso es pertinente reflexionar sobre el consentimiento en la realidad actual.

El objetivo del presente artículo es analizar la situación desventajosa del titular de datos personales cuando sus datos son tratados por empresas privadas recurriendo a la IA y explorar algunas de las medidas previstas en nuevos instrumentos iberoamericanos de soft law que pueden contribuir a fortalecer al titular promoviendo el respeto de los derechos humanos y de principios éticos. Finalmente, se advierte que aún hay trabajo pendiente en esta materia y se aboga por continuar avanzando, con la participación de todos los actores interesados, hacia la adopción de un marco de gobernanza global para la protección de datos personales en tiempos de auge de la IA.

PALABRAS CLAVE

Protección de datos personales, consentimiento, Inteligencia Artificial, big data, desigualdad, Iberoamérica

ABSTRACT

An area in which the tension between the technological innovation implied in Artificial Intelligence (AI) and the protection of personal data manifests is that of the data subject's consent. In fact, AI challenges the scope and the validity of consent. Nevertheless, it is considered that such consent is still a legally relevant option to enable the lawful processing of personal data by the controller. Therefore, it is pertinent to reflect on consent in the current reality.

This article's objective is to analyze the disadvantageous position of the data subject when his personal data is managed by private corporations using AI, and to explore some of the measures provided for in new Ibero-American soft law instruments that can help strengthening the data subject by promoting respect for human rights and ethical principles. Last, it is observed that there is still pending work in this field, and a call is made to continue moving forward, with the participation of diverse stakeholders, towards the adoption of a global governance framework for personal data protection in the rise of AI.

KEY WORDS

Personal data protection, consent, Artificial Intelligence, big data, inequality, Ibero-America

---

*Artículo de Investigación postulado el 26 de febrero de 2020 y aceptado el 22 de octubre de 2020

**Profesora investigadora en la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas, México. (mercedes.albornoz@cide.edu) orcid.org/0000-0002-0205-4964

SUMARIO

1. Introducción

Los datos personales son información acerca de una persona física, identificada o identificable. Esa persona, titular de los datos personales, debe gozar del derecho a protegerlos. En este sentido, el derecho a la protección de datos personales se ha consolidado actualmente como un derecho humano autónomo[1] que, además, ha sido plasmado en diversos instrumentos normativos. Así, por ejemplo, la Carta de los Derechos Fundamentales de la Unión Europea[2] le dedica el artículo 8, que comienza declarando: "Toda persona tiene derecho a la protección de datos de carácter personal que la conciernan". En el caso de México, desde el año 2009[3] se consagró este derecho a nivel constitucional en el artículo 16,[4] incluyendo los derechos de acceso, rectificación, cancelación y oposición. Ahora bien, aunque en muchos países el derecho del titular a la protección de sus datos personales goza de reconocimiento en el derecho positivo[5] lo cierto es que la exposición del titular a recursos tecnológicos en constante y vertiginosa evolución lo coloca en una situación de vulnerabilidad, susceptible de desafiar la efectividad del marco jurídico protector.

[1] La autonomía es especialmente relevante con respecto al derecho a la vida privada y el derecho a la privacidad. Sobre las relaciones y la delimitación entre estos dos derechos y el derecho a la protección de datos personales, ver Maqueo Ramírez, María Solange, Moreno González, Jimena y Recio Gayo, Miguel, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", Revista de Derecho (Valdivia), Universidad Austral de Chile, Facultad de Ciencias Jurídicas y Sociales, Vol. XXX, No. 1, junio 2017, p. 79 y ss.

[2] 2000/C 364/01, Diario Oficial de las Comunidades Europeas: 18 de diciembre de 2000.

[3] Anteriormente, la protección de datos personales no era en México un derecho fundamental y su reconocimiento era de carácter sectorial. García González, Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", Boletín Mexicano de Derecho Comparado, Instituto de Investigaciones Jurídicas, UNAM, nueva serie, Año XL, No. 120, septiembre-diciembre 2007, p. 772.

[4] Constitución Política de los Estados Unidos Mexicanos, párrafo adicionado al artículo 16, Diario Oficial de la Federación: 1° de junio de 2009.

[5] Según Graham Greenleaf, a enero de 2019, eran 132 los países que contaban con legislación en la materia. "Global Data Privacy Laws 2019: 132 National Laws & Many Bills" Privacy Laws & Business International Report, No. 155, 2019, pp. 14-18. [Consultado 20 febrero 2020], Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593, 8 febrero 2019

A esta circunstancia se suma la voracidad de un puñado de grandes empresas –*data brokers* como Google, Apple, Facebook, Amazon– que desarrollan y/o que operan con tecnología de punta para el tratamiento de datos personales, para acceder a los datos de los individuos. Semejante apetito se explica por el hecho de que, en la economía digital, los datos personales son económicamente valiosos[6] en tanto y en cuanto su tratamiento –así como su asociación con otros datos existentes y la inferencia de datos nuevos– permite elaborar perfiles, predecir conductas e incidir en el comportamiento de las personas[7]. En efecto, quien cuente con acceso masivo a datos personales estará en una mejor posición al momento de tomar decisiones, lo que puede traducirse en la obtención de un mayor lucro. En este contexto, en el cual ya se habla de un "capitalismo de datos",[8] la Inteligencia Artificial (en adelante, IA), que suele estar vinculada con el *big data* y no se detiene ante las fronteras estatales, lleva el tratamiento automatizado de datos personales hasta extremos sorprendentes, inimaginables pocos años atrás.

A pesar de que la IA y la innovación tecnológica que ella supone pueden tener efectos muy positivos para las personas, también generan riesgos de vulneración de sus derechos humanos, como el derecho a no ser discriminadas, o el derecho a la protección de los datos personales. Este último derecho entra en tensión con la IA, lo que puede percibirse en relación con el consentimiento del titular para el tratamiento de sus datos personales utilizando IA.

Se afirma que el desarrollo alcanzado por Internet y, particularmente, por la IA, desafía el alcance y la validez de dicho consentimiento[9]. Así, es factible

---

[6] Es claro que "el valor económico otorgado a la información de las personas no radica en el dato por sí mismo, sino en el tratamiento, asociación con otros datos y utilidad que se le dé". Mendoza Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", Revista IUS (México), Instituto de Ciencias Jurídicas de Puebla, nueva época, Vol. 12, No. 41, enero-junio 2018, p. 269.

[7] Por ejemplo, la hoy inexistente empresa Cambridge Analytica, protagonista de un escándalo con impacto en varios países, declaraba en su propio sitio de Internet que usaba datos para "cambiar el comportamiento de la audiencia", ya que conociendo mejor al electorado se logra "una mayor influencia". Risso, Linda, "Harvesting your Soul? Cambridge Analytica and Brexit", en Jansohn, Christa, Brexit Means Brexit? The Selected Proceedings of the Symposium, Akademie der Wissenchaften und der Literatur, Mainz, 6-8 December 2017, Mainz, Akademie der Wissenchaften und der Literatur, 2018, p. 75. Ver Isaak, Jim y Hanna, Mina J., "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", Computer, IEEE Xplore Digital Library, Vol. 51, No. 8, agosto 2018, pp. 56-59. [Consultado 20 febrero 2020], Disponible en: https://ieeexplore.ieee.org/abstract/document/8436400

[8] Myers West, Sarah, "Data Capitalism: Redefining the Logics of Surveillance and Privacy", Business & Society, Vol. 58, No. 1, 2019, pp. 20-41.

[9] Ver, por ejemplo, Cotino Hueso, Lorenzo, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", Dilemata. Revista Internacional de Éticas Aplicadas, Año 9, No. 24, mayo 2017, p. 145. [Disponible para su descarga a partir de: https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104] [Consultado 20 febrero 2020]

preguntarse si, en realidad, el titular puede comprender lo que acepta y/o si su elección es verdaderamente libre. Sin embargo, tanto en el derecho de los Estados latinoamericanos como en el Reglamento europeo de protección de datos personales (en adelante, GDPR)[10] –que detonó una ola de reformas legislativas de este lado del Atlántico–, el consentimiento del titular conserva en la actualidad un papel significativo para habilitar el tratamiento lícito de datos personales por el responsable.

El objetivo del presente artículo es analizar la situación desventajosa del titular de datos personales cuando sus datos son tratados por grandes empresas privadas recurriendo a la IA y explorar algunas de las medidas previstas en dos nuevos instrumentos de *soft law* aprobados por la Red Iberoamericana de Protección de Datos Personales (en adelante, la Red)[11] que pueden contribuir a fortalecer la protección al titular promoviendo el respeto de los derechos humanos y de principios éticos en el tratamiento de datos personales. El propósito de este texto consiste, por lo tanto, en realizar un análisis de la problemática y una indagación de cómo es posible encararla con las herramientas jurídicas actualmente disponibles en Iberoamérica.

En consecuencia, se aborda la posición del titular de datos personales con respecto al tratamiento de estos efectuado por poderosos agentes privados, estudiando instrumentos jurídicos recientes a la luz de la doctrina y cuando se lo estima apropiado, también de sentencias. Asimismo, en atención a la ausencia de un tratado internacional de alcance universal que sea jurídicamente vinculante para la mayoría de los Estados que componen la comunidad internacional, se adopta una perspectiva iberoamericana, sin perjuicio de referencias adicionales a algunas fuentes de otras latitudes. Nótese que la elección de un enfoque regional no implica desconocer el carácter global de la manera en que opera la IA. En cuanto a la doctrina consultada, no se limita a Iberoamérica, sino que también incluye literatura de Estados Unidos y demás países europeos –más allá de España–.

[10] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Diario Oficial de la Unión Europea: 4 de mayo de 2016, L 119.

[11] Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial y Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial. Ambos instrumentos fueron aprobados el 21 de junio de 2019 en Naucalpan de Juárez, México. [Consultadas 20 febrero 2020], Disponibles (respectivamente) en: https://www.argentina.gob.ar/sites/default/files/recomendaciones-generales-para-el-tratamiento-de-datos-en-la-ia.pdf y https://www.argentina.gob.ar/sites/default/files/orientaciones_especificas_de_proteccion_de_datos_en_inteligencia_artificial.pdf

Antes de comenzar, es necesario formular dos advertencias. En primer lugar, las páginas que siguen dan por sentado que el lector ya está familiarizado con nociones jurídicas básicas en materia de protección de datos personales. En segundo lugar, el tratamiento de datos personales llevado a cabo por las autoridades estatales u otros sujetos de naturaleza pública empleando IA es excluido de este trabajo, pues, a pesar de tener muchos puntos de convergencia con el que efectúan los particulares, también plantea otros retos específicos. Por esta razón, cuestiones atinentes al interés público, la seguridad pública, vigilancia masiva, ciudades inteligentes y gobierno electrónico no son abordadas aquí, sin perjuicio de que puedan ser interesantes como objeto de análisis en futuros trabajos.

A continuación, se estudia la IA y su impacto en materia de datos personales. Luego, se analiza el consentimiento para el tratamiento de datos personales y, posteriormente, se exponen las razones para considerar al titular como parte débil. Después, partiendo de la problemática de la vulnerabilidad del titular de datos personales ante los avances de la IA, se procede a explorar algunas medidas susceptibles de ayudar a establecer un equilibrio. Finalmente, se presentan algunas observaciones conclusivas.

2. Inteligencia Artificial y datos personales

En el prólogo del informe de la CNIL (*Commission nationale d'informatique et des libertés*), de Francia, dedicado a cuestiones éticas de los algoritmos y de la IA, la presidenta afirma que la IA "es el gran mito de nuestro tiempo".[12] Ese mito se nutre de visiones apocalípticas que anuncian que el ser humano será superado por las máquinas e, incluso, que las máquinas podrían volverse contra el hombre.[13] Esto demuestra que es conveniente precisar qué se entiende por IA, antes de abordar su relación con los datos personales y la regulación jurídica de dicha relación.

[12] Falque-Pierrotin, Isabelle, "Préface", en CNIL, Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la Loi pour une République numérique, Paris, CNIL, 2017, p. 2. [Consultado 20 febrero 2020], Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

[13] CNIL, Comment permettre..., *op. cit.* nota 12, p. 19.

2.1. ¿Qué es la IA?

Prácticamente siete décadas han pasado desde que Alan Turing se preguntara si las máquinas podían pensar[14] y desde la conferencia de Dartmouth de 1956, cuando John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon usaron el novedoso término "IA"[15]. Según estos últimos, "el aprendizaje y toda otra característica de la inteligencia humana pueden ser descriptos con un nivel de precisión tal, que se podría hacer que una máquina los simulara".[16] Entonces, la cuestión sería "cómo hacer que las máquinas usen lenguaje, creen abstracciones y conceptos, resuelvan tipos de problemas ahora reservados a los seres humanos y se mejoren a sí mismas".[17]

Para tal fin, la IA se vale de algoritmos. Un algoritmo es "la descripción de una secuencia de pasos (o instrucciones) finita e inequívoca que permite obtener un resultado a partir de los elementos suministrados como entrada".[18] El algoritmo clásico, en el cual las instrucciones para que una computadora realice ciertas actividades imitando la inteligencia humana se presentan en lenguaje informático, se caracteriza por ser determinista –es decir, "sus criterios de funcionamiento son explícitamente definidos por quienes lo implementan".[19]– En cambio, la IA basada en *machine learning* trabaja con algoritmos de aprendizaje, probabilísticos, diseñados para ir evolucionando y para ir construyendo los modelos que van a aplicar, en función de los datos que les son suministrados.[20] De este modo, se aprecia que el *machine learning* "constituye (...) una ruptura con respecto al algoritmo clásico".[21]

Asimismo, vale la pena mencionar la distinción entre IA débil e IA fuerte, formulada por John Searle en 1980: en la primera, la computadora es una poderosa herramienta para el estudio de la mente, mientras que en la segunda, la computadora programada de manera adecuada es una mente, pues puede comprender y tener otros estados cognitivos.[22] La IA débil o estrecha puede

[14] Turing, Alan M., "Computing Machinery and Intelligence", Mind, Vol. 59, No. 236, octubre 1950, pp. 433-460. [Consultado 20 febrero 2020], Disponible en: http://www.jstor.org/stable/2251299

[15] McCarthy, John, Minsky, Marvin L., Rochester, Nathaniel y Shannon, Claude E., 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence', 31 agosto 1955. [Consultado 20 febrero 2020], Disponible en: http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

[16] *Ídem.*

[17] *Ídem.*

[18] CNIL, Comment permettre..., *op. cit.* nota 12, p. 15.

[19] *Ibidem*, p. 18.

[20] *Ibidem*, pp. 16 y 18.

[21] *Ibidem*, p. 18.

[22] Searle, John R., "Minds, Brains and Programs", The Behavioral and Brain Sciences, Vol. 3, No. 3, 1980, p. 417.

realizar una o varias tareas específicas; en cambio, la IA fuerte o general es capaz de efectuar la mayor parte de las actividades que los seres humanos pueden llevar a cabo. La IA estrecha, cuyo desarrollo no ha sido lineal, conoce una época de esplendor en el siglo XXI, dada la enorme disponibilidad de datos y la potencia de las herramientas tecnológicas para su tratamiento.[23] A pesar de que aún no ha sido factible desarrollar la IA general, hay autores que vislumbran la superinteligencia artificial –capaz de superar la inteligencia humana– y la consideran alcanzable.[24]

Una de las definiciones más recientes de IA es la elaborada en 2019 por el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial creado por la Comisión Europea,[25] para efectos de los entregables del grupo. Se la concibe, por un lado, como sistema y, por otro lado, como disciplina científica, en los términos siguientes:

> Los sistemas de inteligencia artificial (IA) son sistemas de *software* (y posiblemente también de *hardware*) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno a través de la adquisición de datos, interpretando los datos estructurados o no estructurados recopilados, razonando sobre el conocimiento o procesando la información derivada de esos datos y decidiendo la mejor acción (o las mejores acciones) a seguir para lograr el objetivo determinado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico y también pueden adaptar su comportamiento analizando cómo se ve afectado el entorno por sus acciones previas.
>
> Como disciplina científica, la IA incluye varios enfoques y técnicas, como el *machine learning* (de los cuales el *deep learning* y el *reinforcement learning* son ejemplos específicos), el *machine reasoning* (que incluye planificación, programación, representación del conocimiento y razonamiento, búsqueda y optimización) y robótica (que incluye

[Consultado 20 febrero 2020], Disponible en: https://www.law.upenn.edu/live/files/3413-searle-j-minds-brains-and-programs-1980pdf

[23] CNIL, Comment permettre..., *op. cit.* nota 12, p. 16.

[24] Ver, por ejemplo: Sotala, Kaj, "How Feasible is the Rapid Development of Artificial Superintelligence?", Physica Scripta, Vol. 92, No. 11, noviembre 2017, No. de identificación del artículo: 113001.

[25] Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, A Definition of AI: Main Capabilities and Disciplines. Definition developed for the purpose of the AI GLEG's deliverables, 8 abril 2019, 9 pp. [Consultado 20 febrero 2020], Disponible en: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

> control, percepción, sensores y actuadores, así como la integración de todas las demás técnicas en sistemas ciber-físicos).[26]

Todo lo anterior pone en evidencia la importancia de los datos como insumo para la IA, ya que las decisiones que un sistema de IA tome dependerán del "combustible" utilizado para echar a andar la máquina. Asimismo, el desarrollo tecnológico logrado en la última década permite recolectar y tratar datos masivamente –lo que se conoce como *big data*–. La relación entre IA y *big data* es bidireccional, en el sentido de que la IA necesita enormes cantidades de datos y de que el *big data* utiliza técnicas de IA para extraer valor de los datos.[27] Es más, mientras que "los métodos analíticos tradicionales requieren ser programados para encontrar conexiones y vínculos, la IA aprende de todos los datos que ve (...) y ajusta sus análisis sin intervención humana".[28] Por consiguiente, contribuye a la eliminación de obstáculos técnicos a los cuales se enfrentan los métodos tradicionales al analizar *big data*.[29]

El *big data* "no solamente designa cantidades inmensas de datos diversos sino, igualmente, las técnicas[30] que permiten tratarlos, hacerlos hablar, identificar en ellos correlaciones inesperadas o incluso conferirles capacidad predictiva".[31] Además de las consabidas "3 V" –volumen, variedad, velocidad–, el *big data* se caracteriza por lo que Kenneth Cukier y Viktor Mayer-Schoenberger han denominado *datafication*: "la capacidad de transformar en datos muchos aspectos del mundo que nunca antes habían sido cuantificados".[32] De manera que el uso del *big data* implica un cambio profundo en cómo se trata la información. En lugar de enseñarle a una computadora a hacer algo, se la alimenta masivamente con datos, para que pueda inferir probabilidades.[33] En efecto, se automatiza "tanto el objeto como el procedimiento del conocimiento".[34]

---

[26] *Ibidem*, p. 6. Traducido del inglés por la autora. *Nota bene:* algunos términos permanecen en inglés porque así se los emplea también en la literatura en otros idiomas.

[27] ICDPPC, Artificial Intelligence, Robotics, Privacy and Data Protection. Room document for the 38th International Conference of Data Protection and Privacy Commissioners, Marrakech, octubre 2016, p. 4. [Consultado 20 febrero 2020], Disponible en: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

[28] The Norwegian Data Protection Authority, Artificial Intelligence and Privacy Report, enero 2018, p. 5. [Consultado 20 febrero 2020], Disponible en: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

[29] *Ídem*.

[30] Por ejemplo, la minería de datos o data mining, que permite buscar correlaciones entre los datos. Gil, Elena, Big data, privacidad y protección de datos, Madrid, Agencia Española de Protección de Datos, 2016, p. 99.

[31] CNIL, Comment permettre..., *op. cit.* nota 12, p. 18.

[32] Currier, Kenneth y Mayer-Schoenberger, Viktor, "The Rise of Big Data. How It's Changing the Way We Think About the World", Foreign Affairs, Vol. 92, No. 3, mayo-junio 2013, p. 29.

[33] *Ídem*.

[34] Cotino Hueso, L., *op. cit.* nota 9, p. 132.

2.2. ¿Cómo se relaciona la IA con los datos personales?

De acuerdo con lo referido en el apartado anterior, se percibe que "la IA se basa, inevitablemente, en el tratamiento de datos".[35] Al igual que lo que sucede con respecto al *big data*, los datos que constituyen la materia prima de la IA no siempre son datos personales. Sin embargo, dado que en muchas ocasiones lo son, el vínculo entre la IA y los datos personales es muy estrecho.

Efectivamente, los datos personales son un componente importante del aludido "combustible" que la IA precisa para funcionar. Por eso hay que tener en cuenta que cuando existe recolección de datos personales –más aún si ésta se realiza de forma masiva–, el derecho a la protección de esos datos siempre está en juego.[36] Las empresas que operan como *data brokers* y utilizan herramientas de IA, generalmente emplean como insumos datos personales de los individuos que contratan con ellas, a fin de tomar decisiones automatizadas que inciden en la realidad cotidiana de las personas. Así, por ejemplo, es factible determinar, sin intervención humana en el proceso de decisión, que una persona no es candidata elegible para obtener un crédito, una póliza de seguro o un puesto de trabajo; pero también, qué avisos publicitarios recibirá y qué contenidos verá en línea.[37]

A ello se añaden las inferencias y predicciones de preferencias y conductas que los sistemas de IA pueden realizar, junto a la posibilidad de servirse de los datos personales para influir en el comportamiento de los titulares. Además, los algoritmos inteligentes pueden haber sido diseñados –incluso involuntariamente– con sesgos que incidirán en el resultado final[38]. Las preocupaciones que estas situaciones originan se suman a las más generales sobre seguridad y confidencialidad de la información. También son acentuadas por el velo de

---

[35] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), Artificial Intelligence and Data Protection: Challenges and Possible Remedies, Informe sobre Inteligencia Artificial preparado por Alessandro Mantelero, T-PD(2018)09Rev, p. 5. [Consultado 20 febrero 2020], Disponible en: https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

[36] Oostveen, Manon, Protecting Individuals Against the Negative Impact of Big Data. Potential Limitations of the Privacy and Data Protection Law Approach, Alphen aan den Rijn, Kluwer Law International, Information Law Series, 2018, Vol. 42, p. 53.

[37] Tene, Omer y Polonetsky, Jules, "Big Data for All: Privacy and User Control in the Age of Analytics", Northwestern Journal of Technology and Intellectual Property, Vol. 11, No. 5, 2013, p. 252.

[38] Acerca de los sesgos en algoritmos de *machine learning*, ver Katyal, Sonia K., "Private Accountability in the Age of Artificial Intelligence", UCLA Law Review, Vol. 66, No. 1, 2019, pp. 54-141, especialmente, pp. 62 y ss. [Consultado 20 febrero 2020], Disponible en: https://www.uclalawreview.org/wp-content/uploads/securepdfs/2018/12/66.1.2-Katyal.pdf

misterio y secreto que suele recubrir los algoritmos, así como por su carácter sofisticado e inaprehensible para el individuo común.

Ciertamente, la IA tiene un impacto positivo en diferentes ámbitos de la vida de las personas.[39] No obstante, también implica riesgos de vulneración de derechos humanos, además de riesgos de tipo ético y social[40] y hasta de debilitamiento de la democracia.[41] Entre los derechos humanos que pueden verse afectados, se encuentran la libertad de expresión,[42] el derecho de toda persona a no ser discriminada[43] y también el derecho a la protección de los datos personales, de interés para efectos del presente artículo.

La IA implica un serio desafío para el derecho del individuo a la protección de sus datos personales, al punto de ponerlo en riesgo de volverse letra muerta, carente de proyección en la práctica. Cuanto mayor sea la cantidad de datos personales recolectados por sistemas de IA, mayor será la probabilidad de afectación para el titular y más difícil será que la anonimización contribuya a protegerlo, considerando que puede ser sorteada por la reidentificación facilitada por el *big data*.[44]

En esta misma línea, es necesario señalar que la IA entra en tensión con varios de los principios que todavía son comúnmente aceptados en materia de protección de datos personales. Si se toman como referencia los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (en adelante, los Estándares) elaborados por la Red,[45] cuando la IA utiliza datos personales como materia prima, pueden afectarse especialmente los principios de legitimación (artículo 11), lealtad (artículo 15), transparencia (artículo 16), finalidad

[39] Es de esperarse que los efectos positivos de la IA vayan en aumento, a medida que la tecnología va avanzando. Ver Castro, Daniel y New, Joshua, The Promise of Artificial Intelligence, Washington D.C., Center for Data Innovation, octubre 2016, p. 46 [Consultado 20 febrero 2020], Disponible en: https://euagenda.eu/upload/publications/untitled-53560-ea.pdf

[40] Alessandro Mantelero propone un modelo para evaluarlos, con un enfoque de derechos humanos. "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", Computer Law & Security Review, Vol. 34, No. 4, agosto 2018, pp. 754-772.

[41] La democracia se debilita cuando los ciudadanos son políticamente manipulados a través de la IA. Ver Maqueo, María Solange y Barzizza Vignau, Alessandra, Democracia, privacidad y protección de datos personales, Ciudad de México, Instituto Nacional Electoral, 2019, Cuadernos de divulgación de la cultura democrática, No. 41, 126 p.

[42] Ver Oostoveen, M., *op. cit.* nota 36, pp. 58-60.

[43] *Ibidem*, pp. 54-57.

[44] Rubinstein, Ira S., "Big Data: The End of Privacy or a New Beginning?" International Data Privacy Law, Vol. 3, No. 2, 2013, p. 77.

[45] Los Estándares fueron aprobados el 20 de junio de 2017 en Santiago de Chile. [Consultados 20 febrero 2020], Disponibles en: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

(artículo 17) y proporcionalidad (artículo 18), todos ellos relacionados con el consentimiento (artículo 12)[46].

A modo de conclusión, la relación entre los datos personales y la IA puede sintetizarse así: los primeros contribuyen en calidad de insumos al funcionamiento de la segunda y ésta, a su vez, estremece los cimientos sobre los cuales se erige en la actualidad la protección jurídica de los primeros.

2.3 ¿Cómo está regulada la relación entre IA y datos personales?

La preocupación por minimizar la afectación del tratamiento automatizado de datos personales en el derecho de las personas a la protección de la información de este tipo que les concierne ya había sido planteada y discutida en diversos ámbitos cuando, en junio de 2017, fueron aprobados los Estándares. Eso permitió que fuese tenida en cuenta al redactar dicho instrumento iberoamericano. En efecto, el artículo 29 de los Estándares aborda el tema de manera muy similar a como lo hace el artículo 22 del GDPR.

La norma iberoamericana establece el derecho del titular a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos, sin intervención humana, en tanto se cumplan dos condiciones: *i.* el tratamiento esté destinado a evaluar ciertos aspectos personales o a analizar o predecir el rendimiento profesional, la situación económica, el estado de salud, las preferencias sexuales, la fiabilidad o el comportamiento del titular y *ii.* Esas decisiones produzcan efectos jurídicos con respecto a él o lo afecten significativamente. El artículo 29 de los Estándares contiene una prohibición general del tratamiento automatizado de datos personales sin participación humana[47] que incluye –aunque no se la mencione expresamente– la elaboración de perfiles, siempre que estén presentes las dos condiciones referidas.

[46] Nótese que, en el sistema jurídico mexicano, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Diario Oficial de la Federación: 5 de julio de 2010) le confiere al consentimiento la calidad de principio (artículo 6). De manera general, acerca de esta ley, ver Tenorio Cueto, Guillermo A. (coord. ed.), Ley Federal de Protección de Datos Personales en Posesión de los Particulares, comentada, Ciudad de México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), octubre de 2019. [Consultado 20 febrero 2020], Disponible en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/LFPDPPP%20Comentada_digital.pdf

[47] La ausencia de intervención humana debe interpretarse como ligada a la toma de decisiones. Por lo tanto, si interviene una persona escaneando datos personales para alimentar el sistema de IA o ejecutando la decisión tomada por éste, pero sin posibilidad de influir en el sentido de la decisión, se debe considerar que ese tratamiento automatizado de datos personales entra en el ámbito de aplicación de la prohibición. Ver comentario de Paul Voigt y Axel von dem Bussche al artículo 22 del GDPR sobre este mismo punto. The EU General Data Protection Regulation (GDPR). A Practical Guide, Cham, Springer International Publishing, 2017, p. 181.

Ahora bien, el mismo artículo prevé tres excepciones a la prohibición: que el tratamiento automatizado *1)* sea necesario para la celebración o la ejecución de un contrato entre titular y responsable, *2)* esté autorizado por el derecho interno de los Estados iberoamericanos o, *3)* se base en el consentimiento del titular (artículo 29.2), el cual deberá ser demostrable, hacer referencia específica al tratamiento automatizado y cumplir con los requisitos establecidos en los Estándares.[48] Cuando se presente la primera o la tercera de las excepciones a la prohibición general, que son las dos que derivan del ejercicio de la autonomía de la voluntad del titular, éste "tendrá derecho a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión" (artículo 29.3). Se observa que esta disposición sobre el derecho a la obtención de intervención humana tiene un alcance limitado, puesto que para ejercer los derechos que confiere, el titular debe ser consciente de que es objeto de decisiones automatizadas. No obstante, en la práctica, muchas de las afectaciones se producen sin que el titular siquiera se entere.[49]

Finalmente, los Estándares se separan un poco del GDPR como fuente de inspiración demostrando singular interés por garantizar el respeto de los derechos humanos, al prohibir que el responsable lleve a cabo tratamientos automatizados de datos personales cuyo efecto sea la discriminación de los titulares (artículo 29.4). Los motivos de discriminación previstos son: el origen racial o étnico, las creencias o convicciones religiosas, filosóficas o morales, la afiliación sindical, las opiniones políticas, los datos relativos a la salud, vida, preferencia u orientación sexual y los datos genéticos o datos biométricos.

3. Consentimiento para el tratamiento de datos personales

El consentimiento del titular de datos personales para que estos sean objeto de tratamiento por parte de un sujeto responsable es uno de los pilares sobre los cuales se ha construido el derecho de protección de datos personales.[50] Dirigido a garantizar el derecho del titular a la autodeterminación informativa,[51] a con-

[48] Ver *infra*, sección 3.2.

[49] En este sentido, pero en alusión al artículo 22 del GDPR: Rubinstein, I. S., *op. cit.* nota 44, p. 79.

[50] De Barrón Arniches, Paloma, "La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)", Cuadernos Europeos de Deusto, No. 61, Bilbao, 2019, p. 55. [Consultado 20 febrero 2020], Disponible en: http://ced.revistas.deusto.es/article/view/1644/1996

[51] La Corte Constitucional Federal alemana se pronunció en 1983 acerca de la autodeterminación informativa y consideró que el libre desarrollo de la personalidad requiere que el individuo goce de protección contra la recolección, el almacenamiento, el uso y la transmisión ilimitados de datos personales. Sentencia del 15 de diciembre de

trolar el uso que se hace de sus datos personales, el consentimiento ha venido gozando de un sitio privilegiado entre las razones que habilitan el tratamiento lícito. No obstante, desarrollos tecnológicos como el *big data* y la IA, que frecuentemente son utilizados en conjunto por grandes empresas particulares dedicadas al tratamiento de información, ponen en tela de juicio el alcance y la validez del consentimiento. Aunque se considera que el consentimiento del titular de datos personales continúa siendo una alternativa jurídicamente relevante para dar paso al tratamiento lícito de datos personales, es innegable que constituye un área en la cual se manifiesta la tensión entre la innovación tecnológica que la IA supone y la protección de datos personales. Por eso, a dos décadas de iniciado el siglo XXI, es pertinente reflexionar sobre el consentimiento.

El consentimiento del titular de los datos personales es una de las bases jurídicas en virtud de las cuales el responsable puede encontrarse legitimado para tratar dichos datos. Así lo reconocen los Estándares en el considerando 17 y también la legislación de los Estados iberoamericanos en materia de protección de datos personales. En consecuencia, cuando un particular esté en posesión de datos personales y cuente con el consentimiento del titular para tratarlos, el tratamiento será lícito, siempre que al manifestarse la voluntad se hayan cumplido ciertos requisitos –que serán presentados más adelante en este mismo apartado–.

3.1. El consentimiento y su relación con otros principios de la protección de datos personales

A pesar de que los Estándares no le atribuyen expresamente al consentimiento el carácter de principio de protección de datos personales,[52] de su articulado surge con claridad la importancia primordial que le confieren. Aunque el consentimiento es regulado más detalladamente a propósito del principio de legitimación, se relaciona con todos los principios acogidos en el instrumento.

No obstante, el consentimiento tiene una vinculación muy estrecha con algunos de ellos, por las siguientes razones:

- *principio de legitimación* (artículo 11): porque el responsable sólo puede tratar los datos personales cuando se presenta alguno de los supuestos

1983 sobre la Ley de Censos de 1983, 1 BvR 209/83. [Consultado 14 octubre 2020], Disponible en: https://www.bundesverfassungsgericht.de/e/rs19831215_1bvr020983.html

[52] A diferencia de la legislación mexicana, que sí lo hace. Ver nota 46.

previstos en el artículo 11 y el primero de ellos consiste en que el titular "otorgue su consentimiento para una o varias finalidades específicas"[53];

- *principio de lealtad* (artículo 15): pues, obviamente, el titular no consiente que sus datos personales sean tratados a través de medios engañosos o fraudulentos, ni ser objeto de discriminación injusta o arbitraria;
- *principio de transparencia* (artículo 16): dado que, para que el titular pueda prestar su consentimiento informado, previamente el responsable debe haberle proporcionado información sobre la existencia y las características principales del tratamiento al que serán sometidos sus datos personales;
- *principio de finalidad* (artículo 17): porque el responsable sólo puede tratar los datos personales para las finalidades determinadas, explícitas y legítimas consentidas por el titular, salvo que concurra alguna causal que habilite un nuevo tratamiento –aunque en este supuesto, la legitimación del responsable ya no se fundaría en el consentimiento– y
- *principio de proporcionalidad* (artículo 18): pues el titular consiente el tratamiento de sus datos personales únicamente para ciertas finalidades y el responsable sólo debe tratar los datos que resulten adecuados, pertinentes y limitados al mínimo necesario para dichas finalidades.

3.2. Noción y requisitos de validez del consentimiento

¿Qué se entiende por "consentimiento" en el marco de los Estándares? ¿Cuáles son los requisitos que debe cumplir para ser válido y de ese modo legitimar el tratamiento de datos personales por parte del responsable? El artículo 2.b de los Estándares define el consentimiento como la "manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen".

Asimismo, el artículo 12 de este instrumento de *soft law* agrega condiciones para el consentimiento, en los siguientes términos:

12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su

[53] Los demás supuestos son situaciones en las que, a pesar de no haber consentimiento del titular para el tratamiento de sus datos, es necesario tratarlos –por ejemplo: para el cumplimiento de una orden judicial, para la ejecución de un contrato del que el titular sea parte, para que el responsable cumpla una obligación legal, por razones de interés público establecidas en la ley–.

consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

12.2. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.

Finalmente, cuando el consentimiento se refiera al tratamiento de datos personales sensibles,[54] deberá ser expreso y constar por escrito (artículo 9.1.c de los Estándares).

Por lo tanto, el consentimiento es la manifestación de voluntad del titular de los datos personales en virtud de la cual acepta y autoriza que sus datos sean tratados por el responsable. En la práctica, se configura como la aceptación del aviso de privacidad. Dicho aviso es el documento donde el responsable le informa al titular que sus datos serán objeto de tratamiento y con qué finalidad o finalidades lo serán.

Los requisitos que el consentimiento del titular debe cumplir para ser válido según los Estándares son los siguientes. El consentimiento debe ser:

- *libre*: la voluntad del titular no debe verse afectada por ningún tipo de vicio. La decisión de consentir debe tomarse con plena libertad, sin haber sufrido manipulación alguna;
- *informado*: la información que el responsable debe poner a disposición del titular tiene que permitir que éste ejerza su derecho a la autodeterminación informativa, conociendo que sus datos personales serán objeto de tratamiento, quién los tratará, con qué finalidad o finalidades determinadas, explícitas y legítimas, si serán comunicados interna o internacionalmente a terceros –en su caso, a quiénes y con qué finalidad–, si existen y cómo funcionan los mecanismos para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad, y de qué manera el responsable obtuvo sus datos personales cuando no haya sido el titular quien se los proporcionó directamente.

[54] El artículo 2.1.d de los Estándares define los datos personales sensibles como "aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física".

Todos estos extremos corresponden al principio de transparencia previsto en el artículo 16 de los Estándares. Además, dicha regla exige que la información que el responsable brinde al titular sea suficiente, fácilmente accesible y esté redactada con lenguaje claro, sencillo, susceptible de ser comprendido sin esfuerzo;

- *específico*: referido a una o varias finalidades concretas, por lo que se relaciona de manera directa con el requisito anterior.[55] En este punto se presenta el desafío de hallar un equilibrio entre el grado de detalle con el que se debe informar la finalidad del tratamiento y la necesidad de no caer en tecnicismos que dificulten o impidan la comprensión de la información;
- *inequívoco*: no debe haber lugar a dudas en cuanto a que el titular de los datos personales presta su consentimiento. El consentimiento debe ser indubitable. En otros términos, no ha de caber la posibilidad de interpretar que no hubo consentimiento;
- *expreso*: el consentimiento debe ser otorgado a través de una declaración o una acción afirmativa clara del titular de los datos personales. Se requiere un consentimiento activo, condición que no se verifica si se lo manifiesta "mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento".[56] Asimismo, cuando el titular autorice el tratamiento de datos personales de naturaleza sensible, además de ser expreso,[57] su consentimiento debe constar por escrito (artículo 9.1.c). Finalmente, con respecto al consentimiento pasivo o tácito, llama la atención que, a pesar de no haber sido acogido por los Estándares, se lo mencione como una opción admisible en las Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección

[55] Efectivamente, el consentimiento se especifica sobre la base de la información que el responsable le proporciona al titular. Acerca de la especificidad del consentimiento, ver Kosta, Eleni, Consent in European Data Protection Law, Leiden, Martinus Nijhoff Publishers, 2013, Nijhoff Studies in EU Law, Vol. 3, pp. 219 y ss.

[56] Así lo resolvió recientemente el Tribunal de Justicia de la Unión Europea (Gran Sala) en un caso relativo a la colocación y la utilización de *cookies* para el tratamiento de datos de usuarios de un sitio de Internet: Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV contra Planet49 GmbH, Asunto C-673/17, sentencia del 1° de octubre de 2019, párrafo 65. [Consultado 14 octubre 2020], Disponible a partir de: https://curia.europa.eu/jcms/jcms/j_6/es/

[57] A fin de comprender mejor los alcances de este requisito se puede consultar a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México, cuyo artículo 8 dispone: "El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos".

de los Datos Personales en los Proyectos de Inteligencia Artificial (en adelante, las Orientaciones), adoptadas por la misma Red[58] y

- *revocable*: el titular que presta su consentimiento para el tratamiento de sus datos personales tiene derecho a revocarlo en cualquier momento. Este requisito o característica del consentimiento va de la mano con el derecho a la autodeterminación informativa.[59] La revocación debe ser alcanzable para el titular, quien, si desea retirar el consentimiento previamente otorgado, debe poder hacerlo mediante mecanismos sencillos, ágiles, eficaces, que no le impliquen erogación alguna.

En este tercer apartado se tomó como instrumento jurídico de referencia el conjunto de Estándares aprobados por la Red, cuya fuente de inspiración fue el GDPR. Ambos instrumentos regulan el consentimiento del titular, que debe obtenerse "con anterioridad a la recogida y a la comunicación"[60] de sus datos personales; es decir, antes del tratamiento.

A continuación, se analiza cómo la realidad contemporánea y sus vertiginosos cambios en tiempos de auge de la IA ponen a prueba el consentimiento.

4. El consentimiento ante el auge de la IA: el titular como parte débil

Cuando los agentes privados que operan como *data brokers* a nivel global combinan la potencia del *big data* y de la IA y utilizan datos personales de los individuos se genera una tensión con varios de los principios comúnmente aceptados en materia de protección de datos personales -los más vinculados con el consentimiento-.[61] Así, la innovación tecnológica desafía el alcance y la validez del consentimiento del titular e instala un escenario propicio para cuestionar su importancia. Además, en este contexto, como se verá a continuación,

[58] Orientaciones, p. 12. También la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de México, admite el consentimiento tácito. Lo hace en el artículo 8, redactado en los siguientes términos: "Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición".

[59] Como lo recuerda Kosta, el derecho a la autodeterminación informativa también implica que el derecho del titular a revocar su consentimiento es irrenunciable. Kosta, E., *op. cit.* nota 55, p. 251.

[60] Tribunal de Justicia de la Unión Europea (Segunda Sala), Fashion ID GmbH & Co. KG contra Verbraucherzentrale NRW eV, Asunto C-40/17, sentencia del 29 de julio de 2019, párrafo 102. [Consultado 14 octubre 2020], Disponible a partir de: https://curia.europa.eu/jcms/jcms/j_6/es/

[61] Ver *supra*, sección 3.1.

el individuo titular se encuentra en una posición de desventaja informativa y también económica.

La literatura ha venido reflejando la situación crítica del consentimiento. Roger Brownsword advierte que la sobrevaloración de dicho concepto puede hacer que la *cultura del consentimiento* se convierta en un *culto al consentimiento* si una comunidad se obsesiona con él y lo toma como *la clave* para una justificación ética y legal del tratamiento, en lugar de concebirlo como un componente de una teoría más amplia, enraizada en los derechos humanos.[62] Bert-Jaap Koops y Ronald Leenes aluden a la "lenta erosión de la privacidad".[63] Ira Rubinstein sentencia que "el modelo del consentimiento informado está quebrado, más allá de cualquier reparación regulatoria".[64] Alessandro Mantelero observa que, en algunas situaciones, el modelo tradicional basado en el consentimiento informado, el principio de finalidad y la idea de que el titular puede controlar efectivamente el tratamiento de sus datos personales, resulta inadecuado en la era del análisis predictivo.[65] Yves Poullet, por su parte, hace un llamado a dejar atrás el consentimiento tal como hoy se lo concibe y sugiere explorar la idea de negociaciones colectivas entre titulares y responsables.[66]

Las razones que justifican que ante la IA se pueda hablar de una crisis del consentimiento en tanto eje central de la legitimación del tratamiento de datos personales atañen principalmente a la desigualdad entre quienes utilizan sistemas de IA para llevar a cabo el tratamiento automatizado de datos personales y los titulares a quienes tales datos conciernen. Esa desigualdad tiene una faceta informativa y otra económica. Ambas pueden tener efectos negativos para el titular de los datos personales.

4.1. Desigualdad informativa

Existe un desequilibrio informativo que deja al titular de los datos personales en una posición de debilidad frente al responsable. En efecto, cuando la

[62] Brownsword, Roger, "The Cult of Consent: Fixation and Fallacy", King's Law Journal, Vol. 15, No. 2, 2004, p. 224.
[63] Koops, Bert-Jaap y Leenes, Ronald, "'Code' and the Slow Erosion of Privacy", Michigan Telecommunications and Technology Law Review, Vol. 12, No. 1, 2005, pp. 115-188. [Consultado 20 febrero 2020], Disponible en: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1114&context=mttlr
[64] Rubinstein, I. S., *op. cit.* nota 44, p. 79.
[65] Mantelero, Alessandro, "The future of consumer data protection in the EU. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics", Computer Law & Security Review, Vol. 30, No. 6, diciembre 2014, pp. 645, 649 y ss.
[66] Poullet, Yves, "Is the general data protection regulation the solution?", Computer Law & Security Review, Vol. 34, No. 4, agosto 2018, p. 776.

innovación tecnológica plasmada en sistemas de IA, con el aporte del *big data* y el *machine learning* se nutre de datos personales y los trata para elaborar perfiles, inferir nuevos datos, predecir preferencias y conductas, la obtención de un genuino consentimiento informado del titular se complica. En consecuencia, por más que desde una perspectiva formal se considere que éste presta su consentimiento, desde una perspectiva sustantiva podría cuestionarse su validez y así, eventualmente, privarse al responsable de legitimación para efectuar un tratamiento lícito. Dicho en otros términos, podría estarse ante un consentimiento de baja calidad.[67]

La manifestación por parte del titular de los datos personales de un consentimiento para el tratamiento de aquellos que verdaderamente reúna todos los requisitos exigidos por los Estándares es un gran reto. Para empezar, porque resulta difícil que el titular que se detenga a leer el aviso de privacidad llegue a comprenderlo cabalmente y a entender sus implicaciones.[68] La política de privacidad suele ser excesivamente larga y estar redactada en lenguaje poco claro,[69] a lo que se suma la complejidad técnica de la información. En tales circunstancias, es poco probable que el titular promedio esté en condiciones de entender las implicaciones que tendrá un aviso de privacidad preparado unilateralmente por el responsable y que su consentimiento sea informado.

Adicionalmente, la vulnerabilidad del titular de los datos personales frente al responsable del tratamiento también se percibe en la capacidad que este último tiene para incidir en la voluntad del primero. El diseño y la arquitectura de la elección, completamente controlados por el responsable,[70] pueden ser usados para manipular al titular a fin de que preste su consentimiento. I. van Ooijen y Helena Vrabec explican que algunas características del contexto en el cual se solicita el consentimiento pueden alentar al titular a tomar decisiones que afectan su privacidad.[71] Indican por ejemplo, que la estrategia de preseleccionar casillas por defecto es efectiva, ya que con frecuencia se las percibe

[67] El consentimiento de baja calidad plantea desafíos en diversas áreas en las cuales se emplea la IA. Por ejemplo, en la de los vehículos conectados y aplicaciones relacionadas con la movilidad. Ver European Data Protection Board, Guidelines 1/2020 on Processing Personal Data in The Context of Connected Vehicles and Mobility Related Applications, versión 1.0, adoptada el 28 de enero de 2020, p. 11, No. 49. [Consultada 20 febrero 2020], Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

[68] Ver Carolan, Eoin, "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review, Vol. 32, No. 3, 2016, p. 469.

[69] De Barrón Arniches, P., *op. cit.* nota 50, p. 50.

[70] Carolan, E. *op. cit.* nota 68, p. 472.

[71] Van Ooijen, I. y Vrabec, Helena U., "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective", Journal of Consumer Policy, Vol. 42, 2019, p. 98.

inconscientemente como recomendaciones, o por aversión a la pérdida.[72] Evidentemente, la influencia deliberada en la voluntad del titular podría acabar con el carácter libre del consentimiento.

Otros dos factores relevantes que muestran la asimetría informativa entre los sujetos involucrados y permiten cuestionar la validez del consentimiento son la opacidad de los algoritmos inteligentes[73] y las amplias posibilidades que ofrece la IA. Por un lado, las empresas que dominan el mercado en el negocio del tratamiento automatizado de datos personales no están dispuestas a dar a conocer sus algoritmos, lo que compromete los principios de transparencia y lealtad. Por otro lado, como los algoritmos inteligentes van aprendiendo de su experiencia con los datos que los alimentan y se van actualizando a sí mismos, la información detallada sobre ellos, las finalidades perseguidas y los resultados esperados que el responsable pudiera brindarle al titular nunca podría estar al día.[74] Más aún, es factible llegar a resultados imposibles de prever.[75] Esto socavaría el supuesto carácter informado y específico del consentimiento y se relaciona con la voracidad de la IA, sobre todo cuando se la combina con *big data*. En efecto, el tratamiento automatizado de datos masivos con algoritmos inteligentes tiende a incorporar cada vez más datos, aunque no sean pertinentes ni se limiten al mínimo indispensable para las finalidades consentidas.

Asimismo, es bastante común que las personas presten poca atención a los avisos de privacidad o que los acepten sin siquiera haberlos leído, como un acto reflejo, sin plena conciencia de lo que están consintiendo. Piénsese en la sobrecarga de información a la que se ve sometido un titular usuario de distintas aplicaciones que emplean IA. Sea que se haya leído el aviso de privacidad o no, se ha observado que la expectativa razonable de privacidad va disminuyendo gradualmente a medida que una persona va incorporando nuevos desarrollos tecnológicos a sus actividades.[76] Lo que se desea es utilizar un servicio u otro de manera inmediata, por lo que hay una propensión a dar el clic con el que se manifiesta el consentimiento, a fin de acceder lo antes posible al servicio requerido, sin preocuparse por salvaguardar los propios datos personales.[77] Este tipo de conducta puede revelar una falta de cultura de la privacidad.

[72] *Idem*, p. 99. Recuérdese, no obstante, que los Estándares requieren que el consentimiento sea activo, al igual que el GDPR y la jurisprudencia del Tribunal de Justicia de la Unión Europea. Ver *supra*, nota 56.
[73] Según Sonia Katyal, éste es uno de los obstáculos centrales para lograr mayor transparencia y rendición de cuentas. *Op. cit.* nota 38, p. 59.
[74] Ver Cotino Hueso, L., *op. cit.* nota 9, p. 145.
[75] Rubinstein, I. S., *op. cit.* nota 44, p. 78.
[76] Koops, B.-J. y Leenes, R., *op. cit.* nota 63, p. 177.
[77] Cotino Hueso, L., *op. cit.* nota 9, p. 145.

Finalmente, existe un aspecto de la innovación tecnológica que no debe ser desdeñado en este contexto y que tiene el potencial de poner en jaque cualquier marco jurídico de protección de los datos personales. Como lo señala Ira Rubinstein, el *big data* "permite la reidentificación de los titulares usando datos no personales, lo que debilita la anonimización como una estrategia efectiva y por lo tanto pone en duda la distinción fundamental entre datos personales y datos no personales".[78] Cuando los datos inicialmente personales y posteriormente anonimizados son objeto de tratamiento no se requiere consentimiento ya que, por hipótesis, no hay ni datos personales ni un titular de los mismos. La posibilidad técnica de volver a asociar los datos a la persona introduce, entonces, una disrupción en el sistema.

4.2. Desigualdad económica

La diferencia de poder económico se percibe con claridad al pensar en la relación entre individuos y *data brokers* con presencia global que tratan masivamente los datos de aquéllos para distintas finalidades y obtienen un lucro, frecuentemente exorbitante.[79] El mercado del tratamiento automatizado de datos personales por particulares que utilizan sistemas de IA se caracteriza por un alto grado de concentración en unas pocas empresas, lo que deja muy poco espacio a pequeños y medianos jugadores, o a personas físicas responsables del tratamiento.[80]

Esa concentración, a su vez, incide en que millones de personas[81] deseen o necesiten[82] disfrutar de servicios básicos de la sociedad de la información que los grandes *data brokers* ofrecen. Ahora bien, el requisito para acceder a tales servicios –por ejemplo, una cuenta de correo electrónico, o espacio para almacenar documentos en la nube– es informarle los datos personales a la empresa

[78] Rubinstein, I. S., *op. cit.* nota 44, p. 77.

[79] Por ejemplo, en el primer trimestre de 2020, Facebook alcanzó beneficios netos de 5,200 millones de dólares, duplicando así sus ganancias y Amazon obtuvo una cifra similar en el mismo período. DW, "Facebook duplica ganancias netas hasta US$5.200 millones", 30 de julio de 2020. [Consultado 14 octubre 2020], Disponible en: https://p.dw.com/p/3gCXX

[80] Cabe tener presente que el desequilibrio económico será menos pronunciado cuando el responsable del tratamiento de los datos personales sea una pequeña o mediana empresa y que podría llegar a ser inexistente en caso de que el responsable sea una persona física. Sin embargo, para efectos del presente artículo, los casos relevantes son aquéllos en los cuales el responsable es uno de los grandes *data brokers* privados.

[81] Como lo señala A. Mantelero, el elemento fundamental del poder de estos "barones de los datos" es justamente el tamaño de las bases de datos que tienen. *Op. cit.* nota 65, p. 650.

[82] En la actualidad, el acceso a ciertos servicios de la sociedad de la información puede ser considerado, en algunos ámbitos, como una necesidad. Consecuentemente, la libertad contractual podría verse restringida.

prestadora del servicio y aceptar sus términos y condiciones, que incluyen una política de privacidad en la que se autoriza el tratamiento con IA. Al ceder sus datos personales, lo que el titular en realidad está haciendo es entregar una contraprestación por el servicio,[83] pagar un precio.[84] En consecuencia, el contrato no es gratuito, sino sinalagmático.[85]

El *data broker*, por su parte, aprovecha la debilidad de múltiples usuarios para alimentar masivamente su sistema de IA y obtener un beneficio económico.[86] En un negocio tan lucrativo como éste, el responsable del tratamiento de datos personales puede no estar dispuesto a privilegiar la protección de los intereses del titular en lugar de los intereses propios. Ello pondría en riesgo el respeto al principio de lealtad previsto en el artículo 15 de los Estándares.

Finalmente, la debilidad del titular de datos personales ante la gran empresa con la cual contrata y las innovadoras herramientas tecnológicas que ésta utiliza para el tratamiento, se acentúa debido a la dimensión global del negocio. En tanto no existan normas internacionalmente uniformes sobre protección de datos personales que, además, contemplen las particularidades de la IA y el *big data*, la vulnerabilidad del titular de datos personales ante las comunicaciones transfronterizas de las cuales sus datos son objeto continuará profundizándose.

4.3. Posibles efectos negativos para el titular de los datos personales

La desigualdad tanto informativa como económica del titular de datos personales con respecto a las grandes empresas privadas responsables del tratamiento lo pone en una situación de vulnerabilidad. Su voluntad puede ser manipulada para autorizar el tratamiento de su información personal. Pero aun

[83] No obstante, también hay que tener en cuenta la naturaleza especial de los datos, se distinguen de otros objetos del patrimonio. Por eso es discutible en qué medida puede hablarse de "propiedad de los datos". Schulze, Reiner, "Contratar en la era digital", Working Papers Jean Monnet Chair on European Private Law, 8/2018, Barcelona, Universitat de Barcelona, p. 8. [Consultado 20 febrero 2020], Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124048/1/WP_2018_8.pdf

[84] Es interesante tener presente que esto ha sido formalmente reconocido en la reciente Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales, que define el precio como "el dinero o una representación digital de valor, pagadero a cambio del suministro de los contenidos o servicios digitales" (artículo 2.7). Diario Oficial de la Unión Europea: 25 de mayo de 2019, L 136.

[85] De Barrón Arniches, P., *op. cit.* nota 50, p. 47.

[86] El titular de los datos personales se ha convertido en parte del producto de este modelo de negocio, pero no percibe las ganancias. Martínez Velencoso, Luz M. y Sancho López, Marina, "El nuevo concepto de onerosidad en el mercado digital ¿Realmente es gratis la App?", InDret No. 1, enero 2018, p. 20. [Consultado 20 febrero 2020], Disponible en: https://indret.com/wp-content/uploads/2018/03/1371.pdf

cuando libremente decide prestar su consentimiento, existe el riesgo de que sus derechos humanos sean conculcados.

El consentimiento para que los propios datos personales sean tratados por *data brokers* utilizando sistemas de IA, manifestado en circunstancias desfavorables como las analizadas más arriba,[87] podría ser tomado como un cheque en blanco para autorizar y encubrir diversas prácticas invasivas de la privacidad, legitimándolas. En tal caso, se aparentaría formalmente actuar de manera lícita, cuando en realidad se estarían realizando operaciones de tratamiento que excederían con creces el alcance del consentimiento del titular.

Esas operaciones de tratamiento tienen el potencial de vulnerar el derecho a la privacidad y a la protección de datos personales y adicionalmente, otros más, como el derecho a no ser discriminado o el derecho a tomar decisiones de manera autónoma,[88] en distintos ámbitos de la vida. Situaciones cotidianas ilustran los posibles efectos negativos del tratamiento automatizado de datos personales, de los cuales a menudo no es consciente el titular.

Así, la constante e invasiva recolección de información por parte de los *data brokers* que escuchan las conversaciones, captan las fotografías tomadas con la cámara del teléfono celular, reconocen el rostro del titular y sus contactos, registran cada búsqueda realizada en Internet, al igual que los desplazamientos del titular, sus compras, preferencias y aversiones, sumada a la combinación de esos datos tratados con sistemas de IA, genera todavía mucha más información acerca de la persona. Las múltiples finalidades para las cuales es factible usar todo este aluvión de información personal pueden llegar a ser perjudiciales para el titular. Por ejemplo, cuando los empleadores usan el sistema de búsqueda de LinkedIn para seleccionar automáticamente candidatos a entrevistar para cubrir una vacante[89], cuando la empresa responsable accede a compartir los datos personales del titular con autoridades –incluso extranjeras–[90] o cuando se intenta influir en la voluntad del usuario de redes sociales para que decida adquirir cierto producto o para que vote por determinado candidato en las elecciones de su país.[91]

[87] Ver *supra*, secciones 4.1 y 4.2.

[88] La autonomía implica no sólo que la persona pueda tomar sus propias decisiones, sino que pueda hacerlo "con base en su reflexión personal, más que por influencia externa". Carolan, E., *op. cit.* nota 68, p. 464.

[89] Van Ooijen, I. y Vrabec., H. U., *op. cit.* nota 71, p. 96.

[90] Como sucedió en el caso que culminó con la declaración de invalidez del Escudo de Privacidad Unión Europea-Estados Unidos. Tribunal de Justicia de la Unión Europea (Gran Sala), Data Protection Commissioner contra Facebook Ireland Ltd. y Maximilian Schrems, Asunto C-311/18, sentencia del 16 de julio de 2020. [Consultado 14 octubre 2020], Disponible a partir de: https://curia.europa.eu/jcms/jcms/j_6/es/

[91] Recuérdese el caso Cambridge Analytica. Ver *supra*, nota 7.

En conclusión, el titular es la parte débil frente a la empresa *data brokers* que utiliza IA para el tratamiento de los datos personales de sus clientes. Es cierto que su consentimiento continúa siendo una de las bases de legitimación del tratamiento. Sin embargo, no debe ser visto como objeto de culto. Al contrario, se considera que, por un lado, no hay que perder de vista que existen además otras bases alternativas y que, por otro, es necesario poner en marcha mecanismos adicionales que contribuyan a fortalecer su posición para contribuir a garantizar el derecho a la protección de los datos personales.

5. Medidas para fortalecer la posición del titular de datos personales

La amplia penetración de la IA en la vida de las personas trae consigo nuevos desafíos en materia de protección de datos personales. En particular, ha puesto en crisis al consentimiento y ha obligado a repensarlo, dado que ya no goza de la misma eficacia que se le atribuía hace unos años. El nuevo escenario muestra al individuo titular de datos personales como parte débil en relación con los *data brokers* que emplean su información personal en calidad de materia prima para sus sistemas de IA.

Si bien los Estándares tienen naturaleza de *soft law*, puede afirmarse que reflejan cierto consenso regional con respecto al consentimiento. Por eso se sostiene que, en el momento actual, más que eliminar el consentimiento, es pertinente pensar cómo ir reduciendo su protagonismo en la práctica y en la esfera en la que continúa operando, cómo dotarlo de solidez. El punto de partida es recordar que el consentimiento no es la única base de legitimación del tratamiento. Pero, además, se requiere implementar medidas proactivas que contribuyan al fortalecimiento del titular y a garantizar el pleno ejercicio de sus derechos humanos –especialmente, el derecho a la protección de los datos personales–. Esa tarea debe llevarse a cabo teniendo siempre presente el carácter central del ser humano en el desarrollo de la IA, de manera que este último no sea impulsado por "interés puramente económico o eficiencia algorítmica deshumanizante".[92] Corresponde en cambio, reafirmar la importancia de los derechos humanos y de valores éticos.

Se considera que dentro del ámbito que el consentimiento del titular conserva para legitimar el tratamiento de datos personales con recurso a la IA, aquellas medidas deberían estar encaminadas a apuntalarlo en dos sentidos.

[92] Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), preparado por A. Mantelero, *op. cit.* nota 35, p. 5.

Primero, procurando asegurar que el consentimiento obtenido sea genuino y cumpla con los extremos requeridos por los Estándares.[93] Segundo, tratando de que los principios y derechos en materia de protección de datos sean respetados, independientemente de que la base que legitime el tratamiento sea o no el consentimiento.

Iberoamérica cuenta con dos instrumentos de *soft law* recientemente aprobados por la Red, que se suman a los Estándares y conforman con ellos un incipiente sistema regional de protección de datos personales. Se trata de las Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial (en adelante, las Recomendaciones) y de las Orientaciones.

Las Recomendaciones son diez[94] y están interconectadas, tanto entre sí, como con los Estándares y las Orientaciones. Los Estándares dedican el Capítulo VI a las medidas proactivas en el tratamiento de datos personales, que son las siguientes: privacidad por diseño y privacidad por defecto (artículo 38), oficial de protección de datos personales (artículo 39), mecanismos de autorregulación (artículo 40) y evaluación de impacto a la protección de datos personales (artículo 41). Por su parte, las Orientaciones contienen una sección que se concentra en ofrecer orientaciones específicas para la aplicación de medidas proactivas en el tratamiento de datos personales de los proyectos de IA.[95]

A continuación, se explora la regulación iberoamericana de la privacidad por diseño, la privacidad por defecto y la evaluación de impacto a la protección de los datos personales. Aunque estas medidas no hayan sido introducidas en los Estándares pensando especialmente en la IA, han dado lugar a desarrollos en las Recomendaciones y en las Orientaciones y pretenden contribuir a fortalecer al titular cuyos datos personales son tratados con IA. Es interesante examinar cómo fueron adaptadas, con carácter general y luego con carácter más específico, a la utilización de la IA.

---

[93] *Supra*, sección 3.2.

[94] 1. Cumplir las normas locales sobre tratamiento de datos personales. 2. Efectuar estudios de impacto de privacidad. 3. Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto. 4. Materializar el principio de responsabilidad demostrada (*accountability*). 5. Diseñar esquemas apropiados de gobernanza sobre tratamiento de datos personales en las organizaciones que desarrollan productos de IA. 6. Adoptar medidas para garantizar los principios sobre tratamiento de datos personales en los proyectos de IA. 7. Respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para el ejercicio de los mismos. 8. Asegurar la calidad de los datos personales. 9. Utilizar herramientas de anonimización. 10. Incrementar la confianza y la transparencia con los titulares de los datos personales.

[95] Las orientaciones específicas están agrupadas en secciones. Además de la sección para la aplicación de medidas proactivas, hay otras tres: para el cumplimiento de los principios rectores de la protección de datos personales, para el cumplimiento de las obligaciones por los encargados de tratamiento y para el cumplimiento de los derechos.

De conformidad con el artículo 38.1 de los Estándares, la *privacidad por diseño (o desde el diseño)* consiste en que, desde el diseño del sistema de tratamiento de los datos personales, antes de recabar datos personales, el responsable tome medidas preventivas para la aplicación efectiva de los principios, derechos y demás obligaciones en materia de protección de datos personales previstos en la legislación del Estado iberoamericano que corresponda aplicar.

Una medida relacionada con la privacidad por diseño es la *privacidad por defecto*, contemplada en el artículo 38.2. Esta segunda noción implica que el responsable garantice que todos los sistemas o tecnologías que utilice y que conlleven el tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones establecidos en la legislación aplicable. La misma norma precisa que la privacidad por defecto debe atender específicamente a la minimización de los datos personales objeto de tratamiento y a la limitación de las posibilidades de que un número indeterminado de personas acceda a ellos sin que intervenga el titular.

Las Recomendaciones toman como punto de partida el artículo 38 de los Estándares y lo adaptan al campo de la IA. En este sentido, la recomendación 3 es la de incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto. Con respecto a la privacidad, se considera que para garantizar que en procesos de IA el tratamiento de los datos personales se efectúe de manera correcta, la medida más adecuada es convertir la privacidad en "un componente esencial del diseño y la arquitectura del software o el algoritmo",[96] en un modo predeterminado de operar. Se adopta un enfoque preventivo, a fin de evitar que se produzcan vulneraciones a los titulares. Asimismo, se destaca que es fundamental incorporar la ética y la seguridad en el tratamiento de datos en la IA desde un inicio, al diseñar el sistema y por defecto. Ambas deben irradiar su influjo a todo el esquema, el desarrollo y el uso de productos o procesos de IA.[97]

Por su parte, las Orientaciones agregan la sugerencia de que, cuando se esté desarrollando un sistema de IA, se procure alcanzar los objetivos perseguidos "de una manera menos invasiva para los titulares, en términos de ética, cumplimiento de principios y valorando la relación entre usabilidad y privacidad".[98] También, que se reconozca la importancia de incorporar la privacidad en el diseño y la arquitectura de las tecnologías de IA para que, cuando se haya identificado algún riesgo en materia de privacidad, se propongan medidas

[96] Recomendaciones, p. 16.
[97] Recomendaciones, p. 17.
[98] Orientaciones, p. 39.

técnicas antes de que la vulneración se materialice.[99] Otra orientación específica es la de considerar que los desarrolladores de IA adapten la lógica de los algoritmos para que se permita garantizar la seguridad de los datos personales por defecto y, de esa manera, cumplan con sus obligaciones.[100]

La *evaluación de impacto a la protección de datos personales (o estudio de impacto de privacidad)* es otra medida proactiva que, sumada a la privacidad en el diseño y a la privacidad por defecto, contribuye a colocar al titular en una posición más equilibrada frente al *data brokers*, responsable por el tratamiento de sus datos personales a través de desarrollos tecnológicos que funcionan con IA.

El artículo 41.1 de los Estándares establece, en cabeza del responsable, la obligación de hacer una evaluación del impacto a la protección de los datos personales cuando pretenda realizar un tipo de tratamiento cuya naturaleza, alcance, contexto o finalidades del tratamiento, hagan que sea probable que haya un alto riesgo de afectación del derecho a la protección de los datos personales de los titulares. El estudio de impacto debe realizarse antes de que se llegue a implementar el tratamiento en cuestión. Adicionalmente, en el artículo 41.2, se deja librada a la legislación de los Estados iberoamericanos la indicación de los tratamientos de datos personales que requieran este tipo de evaluación, así como el contenido de la evaluación y en qué circunstancias se la debe presentar ante la autoridad de control competente.

La obligación de hacer una evaluación de impacto es adaptada por las Recomendaciones al tratamiento de datos personales cuando se utiliza IA. Es la recomendación 2 quien la retoma y agrega los rubros que, como mínimo, tal evaluación debería incluir:

- Una descripción detallada de las operaciones de tratamiento de datos personales que involucra el desarrollo de IA;
- Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de datos personales, y
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad, diseño de software, tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas.[101]

[99] Orientaciones, p. 40.
[100] *Ídem.*
[101] Recomendaciones, p. 16.

En cuanto a las Orientaciones, el grado de detalle acerca de diversas cuestiones atinentes a la evaluación de impacto es mayor que el que se aprecia en las Recomendaciones. Una de las orientaciones especifica en qué casos corresponde realizar una evaluación de impacto a la protección de datos personales en el desarrollo de IA. Tales casos son los siguientes: cuando se traten datos personales, o cuando la IA que se utilice pudiera ser percibida como "particularmente intrusiva de la privacidad",[102] o cuando los resultados del empleo de IA "pudieran llevar a la toma de acciones o decisiones con un impacto o afectación a los titulares".[103]

Una orientación adicional añade precisión acerca de los elementos que debe incluir la identificación del riesgo: evaluación de la necesidad de las operaciones de procesamiento en la utilización de IA y su proporcionalidad con respecto a las finalidades perseguidas, identificación de riesgos potenciales para los titulares –abarcando los relacionados con datos sensibles– y evaluación de potenciales riesgos a derechos y libertades de los titulares, en cuanto sean tutelados por la legislación aplicable.[104] Asimismo, las orientaciones proponen que la evaluación se efectúe periódicamente, con la intención de poder mitigar riesgos a propósito de la utilización de la IA y que las evaluaciones queden documentadas, de modo que, en caso de inspecciones o de controversias, puedan ser presentadas ante las autoridades correspondientes.

Finalmente, otro punto que –en un plano más amplio– contemplan las Orientaciones, es la necesidad de involucrar a las diferentes partes interesadas en el ciclo de vida de un sistema de IA, en la solución conjunta de las diferencias que pudieran presentarse entre, por un lado, los principios de protección de datos personales y, por el otro, los requisitos de ese sistema de IA.[105]

6. Observaciones conclusivas

El estudio realizado en el presente artículo muestra que los individuos cuyos datos personales son objeto de tratamiento por parte de grandes empresas particulares que para ello utilizan sistemas de IA, se encuentran en una situación de debilidad. Efectivamente, existe un desequilibrio entre las partes de la relación contractual en virtud de la cual una empresa presta servicios propios de la sociedad de la información y un individuo comparte sus datos personales

[102] Orientaciones, p. 41.
[103] *Ídem.*
[104] *Ídem.*
[105] *Ibidem*, p. 27.

como contraprestación. Esa desigualdad, que tiene una faceta informativa y otra económica, pone en tela de juicio el alcance y la validez del consentimiento en tanto base para sustentar la legitimidad del tratamiento efectuado por los *data brokers* dominantes en el mercado digital. Además, puede derivar en la vulneración de derechos inherentes a la persona, como el derecho a la privacidad, a la protección de los datos personales, a la no discriminación y a tomar decisiones de manera autónoma.

Tomando en cuenta que los Estándares son relativamente recientes y que, a pesar de no ser vinculantes, reflejan cierto consenso regional con respecto al consentimiento, se considera pertinente procurar reducir su protagonismo en la práctica y, en la esfera en la que continúa operando, intentar apuntalarlo con las herramientas disponibles. Cabe aclarar que, por supuesto, esto no implica cerrar la puerta a nuevas figuras que puedan crearse en el futuro.

El punto de partida es tener presente que el consentimiento no es la única base de legitimación del tratamiento. Pero, además, es importante implementar medidas proactivas que contribuyan a fortalecer la posición del titular y a garantizar el pleno ejercicio de sus derechos humanos –en especial, el derecho a la protección de los datos personales–, promoviendo prácticas éticas. En este sentido, se afirma que la privacidad en el diseño y la privacidad por defecto, sumadas a los estudios de impacto de privacidad con respecto a los sistemas de IA, son medidas que pueden contribuir a solucionar el problema de la debilidad del titular de datos personales en su relación con las empresas que operan como *data brokers*.

Ahora bien, la puesta en marcha de tales medidas y en última instancia, la protección de los derechos del titular en el ámbito de la IA, se verían enormemente favorecidas si los *data brokers* fueran conscientes de que invertir en el desarrollo de estrategias específicas en materia de privacidad mejora su imagen corporativa e inspira confianza en los clientes –actuales o potenciales–. Igualmente, tanto la empresa responsable como el titular podrían resultar beneficiados si se invitara a involucrarse en la toma de decisiones atinentes al gobierno de datos, a todos los potenciales afectados por el tratamiento de datos personales mediante el empleo de IA.

Asimismo, sería positivo que los Estados, sus legisladores y autoridades de control u organismos de protección de datos personales intensificaran sus esfuerzos para realizar aportes significativos al desarrollo de una cultura de respeto al derecho a la protección de datos personales, que incorpore valores éticos al utilizar IA. Ello contribuiría a prevenir que los titulares sufran discriminación o que vean restringidas sus libertades en este ámbito.

Finalmente, no hay que olvidar que los *data brokers* que usan datos personales como insumo para la toma automatizada de decisiones operan a nivel global. Por consiguiente, es fundamental poder contar con mecanismos ágiles de cooperación internacional entre autoridades, así como con reglas de gobernanza global en materia de IA y protección de datos personales.

De lo expuesto a lo largo del presente artículo se extrae como conclusión que se debe procurar reducir el carácter protagónico que hasta ahora ha tenido el consentimiento, pero además se debe apuntalar el consentimiento en los ámbitos en los cuales continúe operando como base de legitimación del tratamiento de datos personales con IA, para fortalecer la posición del titular y de ese modo garantizarle protección. Se concluye, asimismo, que aún queda trabajo por delante a fin de continuar desarrollando instrumentos y prácticas ajustados a valores éticos en esta materia. Se aboga por seguir avanzando, con la participación de todos los actores interesados, hacia la adopción de un marco de gobernanza global efectivo para la protección de datos personales en tiempos de auge de la IA.

7. Bibliografía

Brownsword, Roger, "The Cult of Consent: Fixation and Fallacy", King's Law Journal, Vol. 15, No. 2, 2004, pp. 223-251.

Carolan, Eoin, "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review, Vol. 32, No. 3, 2016, pp. 462-473.

Carta de los Derechos Fundamentales de la Unión Europea, 2000/C 364/01, Diario Oficial de las Comunidades Europeas: 18 de diciembre de 2000.

Castro, Daniel y New, Joshua, The Promise of Artificial Intelligence, Washington D.C., Center for Data Innovation, octubre 2016, p. 46. [Consultado 20 febrero 2020] Disponible en: https://euagenda.eu/upload/publications/untitled-53560-ea.pdf

CNIL, Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la Loi pour une République numérique, Paris, Commission Nationale Informatique et Libertés, 2017, p. 2. [Consultado 20 febrero 2020], Disponible en: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

Constitución Política de los Estados Unidos Mexicanos, Reforma que adiciona un párrafo al artículo 16, Diario Oficial de la Federación: 1° de junio de 2009.

Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), Artificial Intelligence and Data Protection: Challenges and Possible Remedies, Informe

sobre Inteligencia Artificial preparado por Alessandro Mantelero, T-PD(2018)09 Rev, p. 5. [Consultado 20 febrero 2020], Disponible en: https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6

Corte Constitucional Federal de Alemania, sentencia del 15 de diciembre de 1983 sobre la Ley de Censos de 1983, 1 BvR 209/83. [Consultado 14 octubre 2020], Disponible en: https://www.bundesverfassungsgericht.de/e/rs19831215_1bvr020983.html

Cotino Hueso, Lorenzo, "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", Dilemata. Revista Internacional de Éticas Aplicadas, Año 9, No. 24, mayo 2017, pp. 131-150. [Consultado 20 febrero 2020], Disponible para su descarga a partir de: https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104

Currier, Kenneth y Mayer-Schoenberger, Viktor, "The Rise of Big Data. How It's Changing the Way We Think About the World", Foreign Affairs, Vol. 92, No. 3, mayo-junio 2013, pp. 28-40.

De Barrón Arniches, Paloma, "La pérdida de privacidad en la contratación electrónica (entre el Reglamento de protección de datos y la nueva Directiva de suministro de contenidos digitales)", Cuadernos Europeos de Deusto, No. 61, Bilbao, 2019, pp. 29-65. [Consultado 20 febrero 2020], Disponible en: http://ced.revistas.deusto.es/article/view/1644/1996

Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales, Diario Oficial de la Unión Europea: 25 de mayo de 2019, L 136.

DW, "Facebook duplica ganancias netas hasta US$5.200 millones", 30 de julio de 2020. [Consultado 14 octubre 2020], Disponible en: https://p.dw.com/p/3gCXX

European Data Protection Board, Guidelines 1/2020 on Processing Personal Data in The Context of Connected Vehicles and Mobility Related Applications, versión 1.0, adoptada el 28 de enero de 2020. [Consultada 20 febrero 2020], Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

García González, Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", Boletín Mexicano de Derecho Comparado, Instituto de Investigaciones Jurídicas, UNAM, nueva serie, Año XL, No. 120, septiembre-diciembre 2007, pp. 743-778.

Gil, Elena, Big data, privacidad y protección de datos, Madrid, Agencia Española de Protección de Datos, 2016, 149 p.

Greenleaf, Graham, "Global Data Privacy Laws 2019: 132 National Laws & Many Bills" Privacy Laws & Business International Report, No. 155, 2019, pp. 14-18. [Consultado 20 febrero 2020], Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593

Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial, A Definition of AI: Main Capabilities and Disciplines. Definition developed for the purpose of the AI

GLEG's deliverables, 8 abril 2019, p. 9. [Consultado 20 febrero 2020], Disponible en: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

ICDPPC, Artificial Intelligence, Robotics, Privacy and Data Protection. Room document for the 38th International Conference of Data Protection and Privacy Commissioners, Marrakech, octubre 2016, p. 4. [Consultado 20 febrero 2020], Disponible en: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

Isaak, Jim y Hanna, Mina J., "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection", Computer, IEEE Xplore Digital Library, Vol. 51, No. 8, agosto 2018, pp. 56-59. [Consultado 20 febrero 2020], Disponible en: https://ieeexplore.ieee.org/abstract/document/8436400

Katyal, Sonia K., "Private Accountability in the Age of Artificial Intelligence", UCLA Law Review, Vol. 66, No. 1, 2019, pp. 54-141. [Consultado 20 febrero 2020], Disponible en: https://www.uclalawreview.org/wp-content/uploads/securepdfs/2018/12/66.1.2-Katyal.pdf

Koops, Bert-Jaap y Leenes, Ronald, "'Code' and the Slow Erosion of Privacy", Michigan Telecommunications and Technology Law Review, Vol. 12, No. 1, 2005, pp. 115-188. [Consultado 20 febrero 2020], Disponible en: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1114&context=mttlr

Kosta, Eleni, Consent in European Data Protection Law, Leiden, Martinus Nijhoff Publishers, 2013, Nijhoff Studies in EU Law, Vol. 3, 441 p.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación: 5 de julio de 2010.

Mantelero, Alessandro, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment", Computer Law & Security Review, Vol. 34, No. 4, agosto 2018, pp. 754-772.

Mantelero, Alessandro, "The future of consumer data protection in the EU. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics", Computer Law & Security Review, Vol. 30, No. 6, diciembre 2014, pp. 643-660.

Maqueo Ramírez, María Solange, Moreno González, Jimena y Recio Gayo, Miguel, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", Revista de Derecho (Valdivia), Universidad Austral de Chile, Facultad de Ciencias Jurídicas y Sociales, Vol. XXX, No. 1, junio 2017, pp. 77-96.

Maqueo, María Solange y Barzizza Vignau, Alessandra, Democracia, privacidad y protección de datos personales, Ciudad de México, Instituto Nacional Electoral, 2019, Cuadernos de divulgación de la cultura democrática, No. 41, 126 p.

Martínez Velencoso, Luz M. y Sancho López, Marina, "El nuevo concepto de onerosidad en el mercado digital ¿Realmente es gratis la App?", InDret No. 1, enero 2018, pp. 1-36. [Consultado 20 febrero 2020], Disponible en: https://indret.com/wp-content/uploads/2018/03/1371.pdf

McCarthy, John, Minsky, Marvin L., Rochester, Nathaniel y Shannon, Claude E., 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence', 31 agosto 1955. [Consultado 20 febrero 2020], Disponible en: http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

Mendoza Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", Revista IUS (México), Instituto de Ciencias Jurídicas de Puebla, nueva época, Vol. 12, No. 41, enero-junio 2018, pp. 267-291.

Myers West, Sarah, "Data Capitalism: Redefining the Logics of Surveillance and Privacy", Business & Society, Vol. 58, No. 1, pp. 20-41.

Oostveen, Manon, Protecting Individuals Against the Negative Impact of Big Data. Potential Limitations of the Privacy and Data Protection Law Approach, Alphen aan den Rijn, Kluwer Law International, Information Law Series, 2018, Vol. 42, p. 247

Poullet, Yves, "Is the general data protection regulation the solution?", Computer Law & Security Review, Vol. 34, No. 4, agosto 2018, pp. 773-778.

Red Iberoamericana de Protección de Datos, Estándares de Protección de Datos Personales para los Estados Iberoamericanos, aprobados el 20 de junio de 2017 en Santiago de Chile. [Consultados 20 febrero 2020], Disponibles en: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

Red Iberoamericana de Protección de Datos, Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial, aprobadas el 21 de junio de 2019 en Naucalpan de Juárez, México. [Consultadas 20 febrero 2020], Disponible en: https://www.argentina.gob.ar/sites/default/files/orientaciones_especificas_de_proteccion_de_datos_en_inteligencia_artificial.pdf

Red Iberoamericana de Protección de Datos, Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial, aprobadas el 21 de junio de 2019 en Naucalpan de Juárez, México. [Consultadas 20 febrero 2020], Disponible en: https://www.argentina.gob.ar/sites/default/files/recomendaciones-generales-para-el-tratamiento-de-datos-en-la-ia.pdf

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Diario Oficial de la Unión Europea: 4 de mayo de 2016, L 119.

Risso, Linda, "Harvesting your Soul? Cambridge Analytica and Brexit", en Jansohn, Christa, Brexit Means Brexit? The Selected Proceedings of the Symposium, Akademie der Wissenchaften und der Literatur, Mainz, 6-8 December 2017, Mainz, Akademie der Wissenchaften und der Literatur, 2018, pp. 75-87.

Rubinstein, Ira S., "Big Data: The End of Privacy or a New Beginning?" International Data Privacy Law, Vol. 3, No. 2, 2013, pp. 74-87.

Schulze, Reiner, "Contratar en la era digital", Working Papers Jean Monnet Chair on European Private Law, 8/2018, Barcelona, Universitat de Barcelona, pp. 1-16. [Consultado 20 febrero 2020], Disponible en: http://diposit.ub.edu/dspace/bitstream/2445/124048/1/WP_2018_8.pdf

Searle, John R., "Minds, Brains and Programs", The Behavioral and Brain Sciences, Vol. 3, No. 3, 1980, pp. 417-457. [Consultado 20 febrero 2020], Disponible en: https://www.law.upenn.edu/live/files/3413-searle-j-minds-brains-and-programs-1980pdf

Sotala, Kaj, "How Feasible is the Rapid Development of Artificial Superintelligence?", Physica Scripta, Vol. 92, No. 11, noviembre 2017, No. de identificación del artículo: 113001.

Tene, Omer y Polonetsky, Jules, "Big Data for All: Privacy and User Control in the Age of Analytics", Northwestern Journal of Technology and Intellectual Property, Vol. 11, No. 5, 2013, pp. 239-273.

Tenorio Cueto, Guillermo A. (coord. ed.), Ley Federal de Protección de Datos Personales en Posesión de los Particulares, comentada, Ciudad de México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), octubre de 2019, p. 271 [Consultado 20 febrero 2020], Disponible en: http://inicio.inai.org.mx/PublicacionesComiteEditorial/LFPDPPP%20Comentada_digital.pdf

The Norwegian Data Protection Authority, Artificial Intelligence and Privacy Report, enero 2018, p. 30 [Consultado 20 febrero 2020], Disponible en: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

Tribunal de Justicia de la Unión Europea (Gran Sala), Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV contra Planet49 GmbH, Asunto C-673/17, sentencia del 1° de octubre de 2019. [Consultado 14 octubre 2020], Disponible a partir de: https://curia.europa.eu/jcms/jcms/j_6/es/

Tribunal de Justicia de la Unión Europea (Gran Sala), Data Protection Commissioner contra Facebook Ireland Ltd. y Maximilian Schrems, Asunto C-311/18, sentencia del 16 de julio de 2020. [Consultado 14 octubre 2020], Disponible a partir de: https://curia.europa.eu/jcms/jcms/j_6/es/

Tribunal de Justicia de la Unión Europea (Segunda Sala), Fashion ID GmbH & Co. KG contra Verbraucherzentrale NRW eV, Asunto C-40/17, sentencia del 29 de julio de 2019. [Consultado 14 octubre 2020], Disponible a partir de: https://curia.europa.eu/jcms/jcms/j_6/es/

Turing, Alan M., "Computing Machinery and Intelligence", Mind, Vol. 59, No. 236, octubre 1950, pp. 433-460. [Consultado 20 febrero 2020], Disponible en: https://www.jstor.org/stable/2251299?seq=1

van Ooijen, I. y Vrabec, Helena U., "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective", Journal of Consumer Policy, Vol. 42, 2019, pp. 91-107.

Voigt, Paul y von dem Bussche, Axel, The EU General Data Protection Regulation (GDPR). A Practical Guide, Cham, Springer International Publishing, 2017, 383 p.