Inteligencia artificial, desinformación y protección de datos personales

Artificial intelligence, misinformation and personal data protection

Dra. Verónica Melo
UFASTA; UCA

RESUMEN

La presencia de la inteligencia artificial en la vida cotidiana supone un cambio social pero también jurídico. Es preciso que el derecho brinde una respuesta y se regulen las implicancias jurídicas de la intervención de robots, bots, androides o cualquier otra denominación que haga referencia a un artefacto dotado de inteligencia artificial, así como también es necesario que se intensifique la tutela de los datos personales en la medida que éstos parecen ser la moneda de cambio en las plataformas online, en especial, las redes sociales. Estamos situados en una época de disrupción tecnológica que interpela al derecho a ofrecer soluciones en todas las áreas, pero especialmente en materia de daños y de protección de datos personales.

PALABRAS CLAVE: inteligencia artificial; fake news; protección de datos personales

ABSTRACT

The presence of artificial intelligence in everyday life represents a social change but also a legal one. It is necessary for the law to provide an answer and regulate the legal implications of the intervention of robots, bots, androids or any other denomination that refers to a device equipped with artificial intelligence, as well as it is necessary to intensify the protection of the personal data to the extent that these seem to be the currency of exchange on online platforms, especially social networks. We are located in a time of technological disruption that challenges the right to offer solutions in all areas, but especially in matters of damage and personal data protection.

KEYWORDS: artificial intelligence; fake news; data protection

Introducción

La presencia de la inteligencia artificial en la vida cotidiana supone un cambio social pero también jurídico. Es preciso que el derecho brinde una respuesta y se regulen las implicancias jurídicas de la intervención de robots, bots, androides o cualquier otra denominación que haga referencia a un artefacto dotado de inteligencia artificial, así como también es necesario que se intensifique la tutela de los datos personales en la medida que éstos parecen ser la moneda de cambio en las plataformas online, en especial, las redes sociales. Estamos situados en una época de disrupción tecnológica[1] que interpela al derecho a ofrecer soluciones en todas las áreas, pero especialmente en materia de daños y de protección de datos personales.

Si tratamos de conceptualizar la inteligencia artificial, debemos explicar que se trata de una designación general utilizada comúnmente para describir un conjunto de conocimientos técnicos y tecnologías relacionadas, incluyendo el aprendizaje automatizado, el análisis predictivo, el procesamiento del lenguaje natural y la robótica[2].

Según el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial creado por la Comisión Europea, la IA puede definirse como un conjunto de sistemas de software (y también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital al percibir su entorno a través de la adquisición e interpretación de datos recopilados, estructurados o no estructurados, razonando sobre el conocimiento o procesando la información derivada de estos datos y decidiendo las mejores acciones a tomar para lograr el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también adaptar su comportamiento mediante el análisis de cómo el entorno se ve afectado por sus acciones anteriores. Como disciplina científica, la IA incluye varias tecnologías, tales como el aprendizaje automatizado (Machine Learning), la planificación, programación, representación del conocimiento, la búsqueda y la optimización de datos, y la robótica (que abarca el control, la percepción, los sensores y los actuadores, así como la integración de todas las demás técnicas en los sistemas ciber-físicos)[3].

El proceso de digitalización condujo a la creación de enormes conjuntos de datos, como una consecuencia de la vida cotidiana. Paulatinamente, cada vez más ámbitos de la vida de las personas se han trasladado al ciberespacio, utilizando *smart phones* todo

[1] Bower, J. L., y Christensen, C. M., (January–February 1995) "Disruptive Technologies: Catching the Wave." *Harvard Business Review* 73, no. 143–53.

[2] Office of the Victorian Information Commissioner (OVIC), Submission in response to the Artificial Intelligencie: Australia´s Ethic Framework Dsicussion Paper, https://ovic.vic.gov.au/wp-content/uploads/2019/06/OVIC-submission-to-DIIS-AI-Ethical-Framework-Discussion-Paper-V1.0-.pdf (consultado el 7/11/2022)

[3] Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial creado por La Comisión Europea en junio de 2018, Directrices Éticas Para Una Ia Fiable, https://urjes.com/pruebas/wp-content/uploads/2021/05/Grupo-independiente-de-expertos-...-Directrices-eticas-para-una-inteligencia-artificial-IA-fiable-ES.pdf (consultado el 7/11/2022)

el tiempo, comprando en línea y compartiendo sus vivencias en las redes sociales. Los datos del consumidor son valiosos. Y es en ese punto donde radica la valuación millonaria de las empresas tecnológicas, a pesar de no cobrar nada a sus usuarios por sus servicios[4].

Todo lo que hacemos a diario genera datos, por ejemplo, buscar en Internet, compartir en las redes sociales, transmitir información al gobierno, como en el caso de la aplicación "Cuidar". De este modo, intencionalmente o no, las personas brindamos grandes cantidades de información sobre nosotros mismos. A medida que la Internet de las cosas (Internet of Things, conocida por su sigla IoT) se propague cada vez más en nuestro entorno físico y espacios personales, el volumen de los datos creados, recopilados y alimentados en los sistemas de IA se profundizará proporcionalmente[5].

En la actualidad, el volumen de los datos personales recopilados, divulgados y utilizados es mucho mayor que en cualquier otro momento de la historia.

Perfilado a partir de la recolección y cruce de datos personales en una sociedad transparente

El perfilado se refiere al proceso de emplear el reconocimiento de patrones y correlaciones para crear perfiles de usuarios que representan o identifican personas.[6]

Estos sistemas de inteligencia artificial constituyen un riesgo para la autonomía de las personas, ya que a partir de los datos empleados, pueden perfilarlas e influir en su comportamiento, sin que los interesados adviertan tal situación[7]. También significan un riesgo a la privacidad desde que permiten la identificación, el monitoreo y seguimiento de las actividades y comportamientos de las personas, tanto en el espacio público como privado[8], ya sea mediante reconocimiento facial y de voz o por medio del seguimiento de sus movimientos a través de los dispositivos inteligentes que llevan consigo.

---

[4] Jablonowska, Agnieszka - Kuziemski, Maciej - Nowak, Anna Maria - Micklitz, Hans-W. - Palka, Przemyslaw - Sartor, Giovanni, "Consumer Law and Artificial Intelligence (Challenges to the EU Consumer Law and Policy Stemming from the Business's Use of Artificial Intelligence), https://cadmus.eui.eu/handle/1814/57484 (consultado el 7/11/2022)

[5] Office of the Victorian Information Commissioner (OVIC), Submission in response to the Artificial Intelligencie: Australia´s Ethic Framework Dsicussion Paper,cit.

[6] Jansen, Philip y Brey, Philip, "Ethical Analysis of AI and Robotics Technologies", http://en.philosophylab.philosophy.uoa.gr/fileadmin/philosophylab.ppp.uoa.gr/uploads/D4.4_Ethical_analysis__AI_R_.pdf (consultado el 28/9/2022)

[7] Sanchez Caparros, Mariana, Los riesgos de la inteligencia artificial para el principio de igualdad y no discriminación. Planteo de la problemática y algunas aclaraciones conceptuales necesarias bajo el prisma del Sistema Interamericano de Derechos Humanos**.,** El dial, Citar**:** elDial.com - DC3045. Publicado el 07/07/2022

[8] Principios Actualizados sobre la Privacidad y la Protecciónde Datos Personales, Organización de los estados americanos, *https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf* (consultado el 28/9/2022)

Estos sistemas inteligentes nos enfrentan a nuevos desafíos éticos y jurídicos desde que pueden afectar el futuro del empleo[9]; el acceso a la información[10], a la democracia y el estado de derecho[11].

Ahora, ¿de qué modo la revolución digital, internet y las redes sociales han transformado la sociedad y las relaciones? Byung Chul Han analiza las diferencias entre la "masa clásica" y la nueva masa, a la que llama el "enjambre digital". Según el autor, se ha formado una nueva masa: el "enjambre digital"[12], que, a diferencia de la masa clásica, el enjambre digital consta de individuos aislados, carece de un nosotros capaz de una acción común, de andar en una dirección o de manifestarse en una voz. Los gigantes tecnológicos se sirven de nuestros intereses (que nosotros mismos damos a conocer) para extraer beneficio de nuestros comportamientos en internet y las redes sociales.

Si Foucault sostenía que los sistemas coercitivos explotaban al ciudadano siguiendo el modelo del panóptico de Bentham (es decir, controlando exteriormente su actividad, observando sin ser observado), ahora han sido sustituidos por un sistema de dominación que, en lugar de emplear un poder opresor, utiliza uno seductor por el que los hombres se someten por sí mismos: gracias a internet las personas se entregan voluntariamente a la observación[13]. Vivimos en un cierto tipo de sociedad en la que estamos al borde de un embotamiento producido por lo que este filósofo llama "el medio digital" y esto podría traer, aparentemente, nuevas formas de alienación y un tipo de comunicación lleno de desencuentros, de pérdida de la sintonía[14]. Según Han: "la comunicación digital se distingue por el hecho de que las informaciones se producen, envían y reciben sin mediación de los intermediarios. No son dirigidas y filtradas por mediadores. La instancia intermedia es eliminada para siempre (...). Medios como blogs, Twitter o Facebook liquidan la mediación de la comunicación, la desmediatizan."[15]

Riesgos para los derechos y libertades de las personas

Existe una estrecha conexión entre la garantía de la privacidad de las personas, especialmente a través del derecho fundamental a la protección de datos personales, y libertad de expresión y derecho a recibir una información veraz. El escándalo Facebook-Cambridge Analytica evidenció una serie de prácticas que habrían afectado, al menos, a cincuenta millones de personas y, sobre cuyos datos personales

[9] Corvalan, Juan Gustavo (2019), *Inteligencia Artificial y trabajo Construyendo un nuevo paradigma de empleo*, Astrea.

[10] Chesney, Bobby y Citron, Danielle, Deepfakes A Looming Challenge for Privacy, Democracy, and National Security, California Law Review [Vol. 107:1753]

[11] Sunstein, Cass, (2001) "Republic.com", *Princeton University Press.*

[12] Han, Byung-Chul, (2014) *En el enjambre*, Barcelona: Herder.

[13] Han, Byung Chul (2013) *La sociedad de la transparencia,* Barcelona: Herder.

[14] Wolton, D. (2010) *Informar no es comunicar. Contra la ideología tecnológica.* Barcelona: Gedisa.

[15] Han, Byung-Chul (2014) *Psicopolítica: Neoliberalismo y nuevas técnicas de poder,* Madrid: Herder Editorial, 33-34.

almacenados por Facebook, se habrían elaborado perfiles individuales con fines de focalización política en la elecciones presidenciales de Estados Unidos de 2016 y en el referéndum sobre la permanencia en la Unión Europea del Reino Unido[16]. En la Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos, se considera constatado que las fugas de datos de usuarios y el acceso concedido a aplicaciones de terceros sirvieron para utilizarse indebidamente en campañas electorales[17]. En el Informe de la Cámara de los Comunes "Disinformation and 'fake news': Final Report" se desarrolla exhaustivamente la cuestión de cómo una posible vulneración del derecho a la protección de los datos personales podría afectar a otros derechos fundamentales, como la libertad de expresión y la libertad de opinión y la posibilidad de pensar libremente sin manipulación[18].

No obstante a que el empleo de datos para otros fines diferentes de aquellos para los cuales fueran recolectados no sea novedoso, la realidad muestra que las posibilidades actuales de micro-segmentación y manipulación online basadas en las tecnologías de big data e inteligencia artificial que permiten la recolección, el almacenamiento, la combinación y el análisis de ingentes cantidades de datos personales hacen que el riesgo para los derechos de las personas sea hoy mucho más real y elevado[19]. Como ha señalado el Supervisor Europeo de Protección de Datos existe una amenaza para los valores democráticos y los derechos fundamentales derivados de la incesante vigilancia a la que son sometidas las personas en el espacio digital por empresas y Estados y, esta disminución de su espacio íntimo tiene como consecuencia un efecto alarmante sobre la capacidad y voluntad de las personas de expresarse y establecer relaciones con libertad, también en la esfera cívica, tan esencial para la salud de la democracia[20].

El fenómeno de la desinformación es complejo, al que contribuyen no solo las noticias falsas, sino también las cuentas falsas y bots, "que amplifican la actividad e intensidad de los servicios"[21], y es posible distinguirlas de un variado elenco de

[16] Wakefield, Jane, Cambridge "Analytica: Can targeted online ads really change a voter's behaviour?", https://www.bbc.com/news/technology-43489408 (consultado el 29/9/2022)

[17] Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos (2018/2855(RSP)),https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_ES.html (consultado el 29/9/2022)

[18] House of Commons Digital, Culture, Media and Sport Committee Disinformation and 'fake news': Final Report Eighth Report of Session 2017–19, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf (consultado el 29/9/2022)

[19] Garriga Dominguez, Ana (2022) "Inteligencia Artificial y el fenómeno de la desinformación: el papel del RGPD y las garantías recogidas en la propuesta de la ley de servicios digitales", en Llano Alonso, Fernando (director), Inteligencia artificial y filosofía del derecho, Laborum ediciones, 451 y ss.

[20] Ídem

[21] Lanier, Jaron, (2018) *Diez razones para borrar tus redes sociales de inmediato*, Barcelona: Debate.

situaciones posibles que abarcarían desde las teorías de la conspiración hasta las informaciones erróneas pasando por las noticias de los medios de comunicación sesgados ideológicamente[22].

En un informe de la Unión Europea del año 2017 se distinguen tres categorías de información distorsionada. En primer lugar, se alude a la desinformación en el sentido de información falsa compartida intencionalmente para causar daño; a continuación se menciona la información errónea con el alcance de información falsa compartida sin la intención de causar daño, y en tercer lugar se refiere a la información maliciosa en la inteligencia de información genuina compartida con la intención de causar daño[23]. Analizando la presente taxonomía, entendemos que las *fake news* quedan englobadas en la primera de ellas, vale decir, en las *fake news* es indispensable la intencionalidad de engañar.

Una de las finalidades de la libertad de expresión es fomentar el autogobierno; una democracia que funcione de forma correcta no puede existir a menos que las personas puedan decir lo que piensan, incluso si lo que piensan es falso. Pero con la ingente difusión de noticias falsas la democracia se resiente, y simultáneamente, nosotros como ciudadanos encontramos dificultades para pensar con claridad sobre cómo reaccionar frente a un problema, no importa la entidad que éste tenga[24].

La libre circulación de opiniones e informaciones se ve obstaculizada por bots y noticias falsas, pero también, cuando se aplican burbujas de filtro, que nos aíslan sin que podamos advertirlo. Al ignorar la forma y los criterios según los cuales los servicios filtran la información que entra y sale, es prácticamente imposible ver lo sesgada que es[25]. Como consecuencia de ello, cuando el entorno online se encuentra personalizado y micro-segmentado, los ciudadanos estamos expuestos a informaciones que refuerzan los sesgos ideológicos y es más difícil encontrar opiniones diferentes, lo que lleva a una mayor polarización política e ideológica.

La polarización de grupos acontece cuando se reúnen personas con afinidades intelectuales, y así terminan defendiendo una versión más extremista que la que sostenían antes de empezar a hablar entre ellos[26]. Supongamos que los miembros de cierto grupo tienden a creer un rumor sobre, por ejemplo, los efectos mortales de una

[22] Allcott, Hunt y Gentzkow**,** Matthew**,** (2017) "Social Media and Fake News in the 2016 Election", 31 J. ECON. PERSP. 211, https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211 (visto el 3/10/2022)

[23] Wardle, Claire Wardle y Derakshan, Hossein, Information Disorder. "Toward an interdisciplinary framework for research and policymaking", 20-21, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (consultado el 27/8/2022)

[24] Sunstein, C. (2014), "On rumors: how to spread falsehoods, why we believe and what to do against them", *Princeton University Press*.

[25] Parisier, Eli, (2017) *El filtro burbuja: Cómo la web decide lo que leemos y lo que pensamos*, Madrid: Taurus.

[26] Stoner, James A. F., A (2008) "Comparison of Individual and Group Decisions Involving Risk", https://www.semanticscholar.org/paper/A-comparison-of-individual-and-group-decisions-risk-Stoner/052446eb36ffdf85466d9a51e3b5960f2010d485 (consultado el 28/12/2021)

vacuna en particular. Es altamente probable que las creencias sobre ese rumor se consolidarán después de que hayan conversado entre ellos. Peor aún, es posible que pasen de ser potenciales creyentes a estar del todo seguros de que ese rumor es verdad, aunque todo lo que sepan es lo que piensan los miembros del mismo grupo. Tengamos en cuenta el papel de Internet y de las redes sociales: cualquiera de nosotros podría recibir abundante información de los demás miembros de un mismo grupo, y al recibirla quizá pensemos que cualquier cosa que nos digan tiene que ser verdad.

En Republic.com, Sunstein llama la atención sobre la potencia de Internet para facilitar que las personas puedan filtrar y descartar la información indeseada. Para el autor, el mercado de las noticias, entretenimiento e información es perfecto: el consumidor puede ver exactamente lo que quiere, es decir, cuando las posibilidades de filtrado son prácticamente ilimitadas, las personas pueden decidir de antemano, y con exactitud, qué es lo que quieren (o no quieren) encontrar; pueden diseñar un universo de comunicaciones a su propio gusto. Esta habilidad es lo que en su momento Nicholas Negroponte denominó The Daily Me (el diario yo)[27].

En este sentido, también el Parlamento Europeo ha analizado los riesgos de la elaboración de perfiles utilizando macrodatos y, entre otras consideraciones, insta a la "Comisión y a los Estados miembros que velen por que las tecnologías basadas en los datos no limiten o discriminan el acceso a un entorno mediático pluralista sino que fomenten la libertad de los medios de información y el pluralismo"[28]. El Supervisor europeo de protección de datos ha identificado en su informe del año 2018 a la difusión humana o algorítmica de fake news entre las amenazas para la autonomía individual, en la medida que debilita la capacidad de los individuos para discriminar entre lo que es información fiable y lo que no lo es[29] y, así también, los procesos democráticos estarían en riesgo de debilitarse a través de las prácticas de marketing político basadas en técnicas de micro-segmentación y elaboración de perfiles psicográficos[30].

Más aún en el contexto del big data, en el que las posibilidades de confección de perfiles con el auxilio de la inteligencia artificial y del machine learning permite inferir las convicciones ideológicas y de conciencia de una persona sin que ésta las haya

[27] Negroponte, Nicholas (1995) *Being digital*, Knopf: Doubleday Publishing Group, 153. El autor se refiere a que cada uno puede crear un Daily me adaptando las noticias que quiere ver de acuerdo a su gusto. Esta predicción de Negroponte del año 1995 la podemos ver realizada por ejemplo cuando algunos sitios web nos presenta artículos sugeridos, basados en nuestro historial de navegación, o en servicios como Paper.li, que selecciona links en las redes sociales de acuerdo a los intereses del usuario.

[28] Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley, texto completo disponible en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_ES.html (consultado el 29/10/2022)

[29] Supervisor europeo de protección de datos, Informe anual 2018 (resumen ejecutivo), https://edps.europa.eu/sites/edp/files/publication/ar2018_executive_summary_es.pdf (consultado el 30/9/2022)

[30] Garriga Dominguez, Ana, "Inteligencia Artificial y el fenómeno de la desinformación: el papel del RGPD y las garantías recogidas en la propuesta de la ley de servicios digitales", cit.

exteriorizado, y hasta podrían hallarse correlaciones que indiquen información sobre la salud, las convicciones políticas, las creencias religiosas o la orientación sexual de las personas.[31]

Desde los albores del reconocimiento a la protección de los datos personales, siempre se enfatizó el carácter instrumental de este derecho, ya que no solamente tutela la autodeterminación informativa sino que garantiza el respeto de otros derechos, en la medida que este derecho protege la libertad de elección de las personas, su derecho a no ser discriminadas y se encuentra directamente engarzada con la propia idea de dignidad y autorrealización humanas.

La ley de protección de datos personales como herramienta para gestionar estos riesgos

La protección de datos es una rama jurídica que está tomando cada vez un rol más destacado en el derecho y se está convirtiendo en un campo jurídico transversal. El abordaje de la protección de datos está evolucionando y se está diversificando en diferentes nuevas especialidades y tipologías de tutela dentro de la protección de datos, tendiendo a obtener una mayor y más eficiente protección de los diferentes derechos que pretende tutelar el campo de la protección de datos.

La evolución del derecho obliga a aplicar una especificidad a los diferentes nuevos derechos que surgen para conseguir una correcta cobertura jurídica. El derecho otorga una prioridad local a las disciplinas especializadas dividiéndolas en ramas y especialidades, las cuales son aplicables para su protección de forma coherente con una seria de leyes o principios del derecho aplicables a dichas especialidades; es decir leyes específicas.[32]

Esta rama del derecho tienes sus inicios modernos a finales del siglo XIX, y ha ido evolucionando y se enfrenta hoy al desafío que le presenta la realidad con el auge de la inteligencia artificial, el data mining y la Internet de las cosas (IoT). La protección de datos es un ámbito que nos interpela a revisarlo dado el contexto tecnológico en el que nos hallamos. El mundo necesita de una regulación en torno a la protección de datos mucho más innovadora, realista e idónea para cumplir su función tuitiva.

Las nuevas técnicas de análisis de datos masivos han cambiado el sentido y el abordaje de los datos, convirtiéndolos en el activo más valioso de las estrategias comerciales. En la actualidad, existen empresas que se dedican a la minería de datos, y así, por ejemplo, colocan su tecnología no intrusiva en espacios comunes de centros comerciales para obtener pulsaciones electromagnéticas que emiten los teléfonos

[31] Tropnikov, Aleksandr Sergeevich, Uglova, Anna Borisovna, Abdullohonovich Nizomutdinov, Boris, "Application of social networks users digital fingerprints to predict their information image. In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance" (ICEGOV 2020). Association for Computing Machinery, New York, 839–842. https://doi.org/10.1145/3428502.3428635, (consultado el 5/11/2022)

[32] Vergara Blanco, Alejandro, "Los jueces en la era del derecho democrático: especialización, principios y activismo judicial", https://repositorio.uc.cl/handle/11534/45713 (consultado el 13/11/2022)

celulares con el objetivo de captar información relevante que, luego de ser cruzada con otros datos enriquecidos, pueda en un futuro ayudar a predecir la demanda, estableciendo nuevos objetivos en la atracción de nuevos y antiguos clientes[33].

El empleo de la información obtenida puede resultar a veces perjudicial en la medida que podría darse una defectuosa correlación de los datos o simplemente porque los datos recolectados y correlacionados se encuentran encuadrados en la esfera privada. De este modo los datos de carácter personal quedarán regulados por las leyes de protección de datos personales, siendo el consentimiento el instrumento indispensable para legitimar el tratamiento de éstos[34].

Las compañías que implementan estas técnicas de recolección y análisis de datos masivos encuentran el consentimiento del titular para realizar estas acciones, ya que a fin de ofrecer algún premio o beneficio o para permitir conectarse a una red wifi o acceder a páginas web, el usuario debe aceptar los términos y condiciones o que la página trabaja con cookies. Así, los datos se han convertido en materia prima de los negocios, con la potencialidad de crear nuevas formas de valor: nada es gratis, la moneda de cambio con que pagamos son nuestros datos.

El consentimiento libre e informado es la base legal que legitima la recolección y procesamiento de los datos y es lo que se erige en condición *sine qua non* para justificar las operaciones de tratamiento de los datos de carácter personal. Toda normativa que gire en torno al consentimiento coloca en cabeza de su titular la responsabilidad de otorgarlo. Hoy parecería que las normas apuntan a mayor transparencia al momento de indicar el objetivo de la recolección, para que de este modo el consentimiento sea prestado de manera informada por el titular[35]. El consentimiento del titular de los datos siempre representó el medio para respetar la autonomía de la persona, su derecho a la privacidad y a la autodeterminación informativa, que es el bien jurídico protegido en la ley de protección de datos personales.

La naturaleza de informado del consentimiento plantea no pocos inconvenientes en este contexto de *big data* ya que frecuentemente es muy difícil confirmar que éste ha sido dado de manera fundada, teniendo cabal conocimiento de lo que se acepta. Esto se vuelve más complejo cuando hablamos de *big data*, no solo por la masividad y la imposibilidad *a priori* de determinar cuál será su destino sino también porque estos datos se originan en diferentes fuentes, asimismo, los datos recolectados para un fin pueden ser reutilizados luego para otro, en la búsqueda de nuevas correlaciones[36]. El hecho de que exista consentimiento del afectado para el tratamiento de sus datos en otros casos no significa que se pueda efectuar un tratamiento paralelo, que supondría una vulneración del principio de finalidad del tratamiento contenido en el artículo 4.1 y

[33] Tedesco, María de los Angeles (2020) *Inteligencia artificial y derecho: un reto social* (director Granero, Horacio), Buenos Aires: Albremática.

[34] Althabe, María Victoria, Big Data: un desafío para el derecho a la privacidad, TR La ley AR/DOC/1513/2022

[35] Ídem

[36] Ídem

4.3[37] de la ley 25.326 de protección de datos personales. La doctrina ha expresado al respecto que "la legitimidad del fin para el cual el responsable de la base de datos los ha obtenido, es lo que otorga justificación al uso de datos personales de terceros y establece un límite a su utilización"[38]. En síntesis, el principio de finalidad impide que los datos sean utilizados indiscriminadamente, incluso cuando hayan sido lícitamente recolectados, toda vez que cuando sean empleados con un propósito diferente, se necesitará un nuevo consentimiento de su titular.

Las problemáticas al consentimiento que ha traído el uso de las nuevas tecnologías han sido receptadas por los operadores jurídicos y entre las soluciones planteadas figura la de requerir que los términos y condiciones en cuanto a la privacidad deben ser redactados de manera sencilla y que utilicen mecanismos que aseguren que el consentimiento sea informado. Pero estos retos son insuficientes cuando pensamos en *big data*.

Las legislaciones más avanzadas han planteado la necesidad de un cambio de paradigma, planteando la privacidad como diseño y por defecto[39]. Lo que implica entender la privacidad desde el momento inicial en la estructuración ante el tratamiento de datos, entendiendo que la primera opción del titular de los datos y la que debe ser por defecto es la de conservar la privacidad, ante todo. Para ello lo que se busca es que la protección de datos sea proactiva y no reactiva[40]. El objetivo sería que la privacidad se vea asegurada en todo el ciclo de vida del dato.

Conclusiones

La inteligencia artificial, junto a otras tecnologías digitales emergentes, tales como la Internet de las cosas (IoT), o la DLT (Distributed Ledger Technology) tienen un impacto positivo sobre la sociedad y la economía actual. No obstante, desde el derecho urge pensar en soluciones que minimicen los daños y las lesiones a los derechos fundamentales que ellas podrían causar. Una vez combinadas con inteligencia artificial, estas tecnologías conminan a redimensionar la idea de la intervención humana en la prestación de servicios o en la fabricación de productos.

En este trabajo hemos dejado planteada la inquietud acerca de cuál sería el modo más idóneo de proteger derechos fundamentales como la libertad de expresión y de información ante la propagación de noticias falsas, así como también cuál sería la

[37] "Artículo 4° — (Calidad de los datos).

1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. (…)

[38] Gozaini, Osvaldo (2001) Hábeas data: protección de datos personales, Rubinzal Culzoni Editores, p.55.

[39] Reglamento (UE) (27 de abril de 2016) 2016/679 del parlamento europeo y del consejo.

[40] Faliero, Johanna, "El anonimato: epítome de la seguridad informática y privacidad en el sistema crypto"., Fintech, 1ra. Edición, segunda reimpresión.

adecuada manera de proteger los datos personales ante el avance de tecnologías intrusivas.

Independientemente de cual vaya a ser la respuesta del derecho respecto del abordaje de las noticias falsas y del tratamiento masivo de datos, es importante tener en cuenta que nos encontramos ante amenazas a derechos fundamentales que reclaman una solución urgente. Por el lado de las noticias falsas, resulta imperioso encontrar una respuesta compatible con los más elevados estándares de respeto de la libertad de expresión. Finalmente, en lo referido a la protección de datos personales, si bien se destaca la importancia de dar protección a los datos personales también se advierte la importancia de garantizar un nivel equivalente a la libre circulación de datos.

Bibliografía

Allcott, Hunt Y Gentzkow, (2017) Matthew**,** "Social Media and Fake News" in the 2016 Election, 31 J. Econ. Persp. 211 https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211 (visto el 3/10/2022)

Althabe, María Victoria, "Big Data: un desafío para el derecho a la privacidad", TR La ley AR/DOC/1513/2022

Bower, J. L., Y Christensen, C. M., (January–February 1995) "Disruptive Technologies: Catching the Wave." *Harvard Business Review* 73, no. 1.

Chesney, Bobby Y Citron, Danielle, "Deepfakes A Looming Challenge for Privacy, Democracy, and National Security", California Law Review Vol. 107.

Corvalan, Juan Gustavo, (2019) "Inteligencia Artificial y trabajo Construyendo un nuevo paradigma de empleo", Astrea.

Faliero, Johanna, "El anonimato: epítome de la seguridad informática y privacidad en el ecosistema crypto", Fintech, 1ra. Edición, segunda reimpresión

Garriga Dominguez, Ana, (2022) "Inteligencia Artificial y el fenómeno de la desinformación: el papel del RGPD y las garantías recogidas en la propuesta de la ley de servicios digitales", en Llano Alonso, Fernando (director), Inteligencia artificial y filosofía del derecho, Laborum ediciones.

Gozaini, Osvaldo, (2001) *Hábeas data: protección de datos personales*, Rubinzal Culzoni Editores.

Han, Byung Chul, (2013) *La sociedad de la transparencia*, Barcelona: Herder.

Han, Byung-Chul, (2014) *En el enjambre*, Barcelona: Herder.

Han, Byung-Chul, (2014) *Psicopolítica: Neoliberalismo y nuevas técnicas de poder*, Madrid: Herder.

Jablonowska, Agnieszka - Kuziemski, Maciej - Nowak, Anna Maria - Micklitz, Hans-W. - Palka, Przemyslaw - Sartor, Giovanni, "Consumer Law and Artificial Intelligence" (Challenges to the EU Consumer Law and Policy Stemming from the Business's Use of Artificial Intelligence), https://cadmus.eui.eu/handle/1814/57484 (consultado el 7/11/2022)

Jansen, Philip y Brey, Philip, "Ethical Analysis of AI and Robotics Technologies", http://en.philosophylab.philosophy.uoa.gr/fileadmin/philosophylab.ppp.uoa.gr/uploads/D4.4_Ethical_analysis__AI_R_.pdf (consultado el 28/9/2022)

Lanier, Jaron, (2018) *Diez razones para borrar tus redes sociales de inmediato,* Barcelona: Debate.

Negroponte, Nicholas, (1995) "Being digital", Knopf Doubleday Publishing Group.

Parisier, Eli, (2017) *El filtro burbuja: Cómo la web decide lo que leemos y lo que pensamos,* Madrid: Taurus.

Documento *"Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, Organización de los estados americanos",*

https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf (consultado el 28/9/2022)

Reglamento (UE) (27 de abril 2016) 2016/679 del parlamento europeo y del consejo.

Resolución del Parlamento Europeo, de 25 de octubre de 2018, sobre la utilización de los datos de los usuarios de Facebook por parte de Cambridge Analytica y el impacto en la protección de los datos (2018/2855(RSP)**),** https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_ES.html (consultado el 29/9/2022)

Sanchez Caparros, Mariana, "Los riesgos de la inteligencia artificial para el principio de igualdad y no discriminación. Planteo de la problemática y algunas aclaraciones conceptuales necesarias bajo el prisma del Sistema Interamericano de Derechos Humanos"**,** elDial.com - DC3045 Publicado el 07/07/2022

Stoner, James A. F., A (2008) "Comparison of Individual and Group Decisions Involving Risk, https://www.semanticscholar.org/paper/A-comparison-of-individual-and-group-decisions-risk-Stoner/052446eb36ffdf85466d9a51e3b5960f2010d485 (consultado el 28/12/2021)

Sunstein, C., (2014) "On rumors: how to spread falsehoods, why we believe and what to do against them", Princeton University Press.

Sunstein, Cass, April (2001) "Republic.com", *Princeton University Press*.

Supervisor europeo de protección de datos, Informe anual 2018 (resumen ejecutivo), https://edps.europa.eu/sites/edp/files/publication/ar2018_executive_summary_es.pdf (consultado el 30/9/2022)

Tedesco, María de los Ángeles (2020) *Inteligencia artificial y derecho: un reto social,* (director Granero, Horacio), Buenos Aires: Albremática.

Tropnikov, Aleksandr Sergeevich, Uglova, Anna Borisovna, Abdullohonovich Nizomutdinov, Boris, "Application of social networks users digital fingerprints to predict their information image. In Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance" (ICEGOV 2020). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3428502.3428635, (consultado el 5/11/2022)

Vergara Blanco, Alejandro, "Los jueces en la era del derecho democrático: especialización, principios y activismo judicial", https://repositorio.uc.cl/handle/11534/45713 (consultado el 13/11/2022)

Wakefield, Jane, Cambridge "Analytica: Can targeted online ads really change a voter's behaviour?", https://www.bbc.com/news/technology-43489408 (consultado el 29/9/2022)

Wardle, Claire Wardle y Derakshan, Hossein, "Information Disorder. Toward an interdisciplinary framework for research and policymaking", https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (consultado el 27/8/2022)

Wolton, D., (2010) *Informar no es comunicar. Contra la ideología tecnológica.* Barcelona: Gedisa.