LA INTELIGENCIA ARTIFICIAL, EL *BIG DATA* Y LA ERA DIGITAL: ¿UNA AMENAZA PARA LOS DATOS PERSONALES?

ANDREA MARTÍNEZ DEVIA*

RESUMEN

La Inteligencia Artificial (IA) es el presente y el futuro de la humanidad, ya que cada vez más dependemos de la tecnología para realizar nuestras actividades diarias. La IA se puede definir como la simulación realizada por máquinas o sistemas informáticos de procesos o de actividades realizadas por la inteligencia humana. En este sentido, el funcionamiento de la IA se basa en el análisis de miles de datos conocidos como *big data*, dentro de los que se pueden encontrar datos de carácter personal, los cuales, por su esencia, deben ser tratados de manera ética, responsable y transparente para proteger los derechos de los titulares.

Para poder asegurar el adecuado tratamiento de los datos personales en la era digital, Colombia deberá adecuar la normativa existente e implementar de esta forma regulaciones adaptadas a las nuevas tecnologías, a fin de que los responsables tengan directrices para realizar un uso correcto de la información personal cuando desarrollen y usen nuevas tecnologías, priorizando la protección de los derechos de los titulares, quienes, a su vez, deberán desempeñar un papel activo respecto de las implicaciones que trae consigo la entrega y la autorización del uso de sus datos en las herramientas de Inteligencia Artificial.

Palabras clave: inteligencia artificial, datos personales, responsabilidad demostrada, mecanismos de protección, protección de datos, privacidad, transparencia.

* Socia de la firma Martínez Devia & Asociados. Abogada de la Universidad de los Andes (2011), máster en Derecho Comparado enfocado a la Propiedad Intelectual de la Universidad California Western School of Law de San Diego en Estados Unidos (2014). Certificada como auditora interna de Sistemas de Gestión de la Seguridad de la Información - ISO 27001:2013 (2017). Contacto: amartinez@martinezdevia.com. Bogotá D. C. (Colombia). Fecha de recepción: 8 de marzo de 2019. Fecha de aceptación: 21 de mayo de 2019. Para citar el artículo: Martínez Devia A. "La inteligencia artificial, el *Big Data* y la era digital: ¿una amenaza para los datos personales?", *Revista La Propiedad Inmaterial* n.º 27, Universidad Externado de Colombia, enero-junio 2019, pp. 5-23. DOI: https://doi.org/10.18601/16571959.n27.01

ARTIFICIAL INTELLIGENCE BIG DATA, AND DIGITAL ERA: A THREAT TO PERSONAL DATA?

ABSTRACT

Artificial Intelligence (AI) is the present and future of humanity, as we increasingly rely on technology to perform our daily activities. The (AI) can be defined as the simulation performed by machines or computer systems of processes or activities carried out by human intelligence. In this sense, the operation of the AI is based on the analysis of thousands of data known as "big data", within these are personal data, which, by their essence, should be treated in an ethical, responsible and transparent way to protect the rights of the owners.

In order to ensure the adequate treatment of personal data in the digital age, Colombia must adapt the existing normative and implement regulations adapted to new technologies, in order that the Responsible have guidelines for the correct use of personal information when develop and use new technologies, prioritizing the protection of the Rights of the Owners, who, at the same time, should exercise an active role regarding the implications that the delivery and authorization of the use of their data in the Artificial Intelligence tools entails.

Keywords: Artificial intelligence, big data, accountability, protection mechanisms, data protection, privacy, transparency.

INTRODUCCIÓN

Desde hace un par de décadas, la tecnología se convirtió en una herramienta importante para el diario vivir, por lo que los seres humanos dependemos cada vez más de ella en diferentes aspectos (transporte, comunicación, educación, salud, entre otros). Además, para muchos negocios es de gran valor, ya que por medio de las herramientas tecnológicas se ha logrado identificar necesidades y comportamientos del consumidor, reducir tiempos en los procesos productivos, aumento en la productividad, facilidad en el acceso y distribución de bienes y servicios, generando así aumentos significativos en sus ingresos.

El mundo no para y cada día contamos con nuevas tecnologías y herramientas tecnológicas que realizan procesos y desarrollos incluso inimaginables para la mente humana. Dentro de las numerosas tecnologías que existen, se destacan las herramientas que hacen parte de la Inteligencia Artificial (IA)[1], entendida como

1 Real Academia Española. Definición inteligencia artificial. *Real Academia Española*. [Citado el 20 de abril de 2019.] https://dle.rae.es/?id=LqtyoaQ. Inteligencia artificial. "Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico".

la simulación de procesos o actividades humanas llevadas a cabo por máquinas dotadas con la capacidad de razonar, planificar y aprender.

La IA implica necesariamente el tratamiento de datos masivos, dentro de los cuales se incluyen diferentes categorías de datos personales por lo que resulta importante un control y una regulación apropiada para el tratamiento de dichos datos personales con el fin de mitigar riesgos para sus titulares. Por esto, para que se pueden aprovechar las nuevas tecnologías de una manera adecuada y ética es imprescindible que los Estados garanticen el cumplimiento del derecho y los principios y derechos fundamentales por medio de la creación de leyes adaptadas a la era digital y nuevas tecnologías.

Actualmente en Colombia no existen reglas claras sobre la materia, lo que lleva a que aquellos que estén tratando los datos, ya sea como responsables o como encargados, pongan sus intereses por encima de los intereses de los titulares. Mediante una regulación clara y adaptada a esta nueva era digital, las compañías que tratan los datos de carácter personal podrán tener conocimiento de los límites a establecer en el tratamiento, el deber de informar a los titulares sobre el tratamiento de los datos y ser más conscientes de las implicaciones que pueda traer el uso de estas tecnologías para estos desde el punto de vista de la privacidad, el consentimiento y la transparencia[2]. Así mismo, los titulares deberán ser más activos en la protección de sus datos y el respeto de sus derechos para que de esta manera exista una articulación entre los tres actores involucrados en el tratamiento: los Estados, las compañías y los titulares.

Este artículo pretende esbozar los lineamientos que se deben implementar en Colombia relacionados con el tratamiento de los datos personales en relación con la IA, esto teniendo en cuenta la experiencia de otros países. Para ello, primero se define, en términos generales, el concepto de IA y su relación con los datos personales, para después realizar un análisis sobre las regulaciones de protección de datos personales existentes en algunos países a nivel internacional y en Colombia. Posteriormente, se indican los riesgos que ha traído el mal uso de los datos personales en las nuevas tecnologías al incluir unos casos particulares, para finalizar con unas conclusiones sobre las regulaciones que se deben implementar en el país y el papel que deben desempeñar los responsables y los titulares de los datos personales.

LA INTELIGENCIA ARTIFICIAL

Cuando se piensa en el término Inteligencia Artificial (IA), lo primero que se viene a la mente es la imagen de un robot o un elemento muy sofisticado y complejo, sin embargo, la IA es más que esto, está presente en muchos recursos que se usan de manera constante en nuestro diario vivir, por ejemplo, los motores de bús-

2 Mayer-Schönberger, V. y Cukier, K. *Big Data. A Revolution That Will Transform How We Live, Work, and Think* (Madrid: Houghton Mifflin Harcourt, 2013), 215.

queda de Google o Yahoo! por medio de los cuales se pueden estudiar hábitos y comportamientos de las personas, así mismo, plataformas como YouTube, Spotify o Netflix que analizan las preferencias para ofrecer películas, series, canciones o vídeos.

La IA funciona con la presencia de dos elementos fundamentales. El primero es el *computing power* que comprende el desarrollo de los sistemas computacionales y sus máquinas que permiten procesar datos y realizar operaciones en tiempos mínimos, ampliando cada vez más la memoria de almacenamiento[3]. El segundo elemento son los macrodatos o *big data*, que alimentan a la IA, que consisten en un gran volumen de datos producidos por diferentes fuentes (humanas, biométricas, máquina a máquina, grandes transacciones, uso de la web, redes sociales, entre otros), que pueden estar estructuradas o no y son procesadas por diferentes herramientas para obtener diversos resultados.

El uso continuo que se hace de distintas tecnologías (webs, aplicaciones, servicios, sensores incorporados en dispositivos, las búsquedas en internet, las redes sociales, computadores portátiles, teléfonos inteligentes, dispositivos GPS, entre otros) ha incrementado la cantidad de información que se almacena cada día.

El volumen de datos que se recolecta actualmente no podría ser analizado por los métodos tradicionales de almacenamiento, acceso y análisis, por esta razón se han desarrollado nuevas herramientas de IA, la implementación de algoritmos y estadísticas mediante las cuales se pueden obtener resultados, tales como el comportamiento de las personas, sus gustos, la toma de decisiones, el reconocimiento de voz, la identificación de objetos, el diagnóstico de enfermedades, el ahorro de energía, la elaboración de perfiles para analizar o predecir aspectos relativos al rendimiento profesional, la situación económica, la salud, los intereses, la fiabilidad, el comportamiento o la ubicación, datos que se utilizan con diversos fines y se encuentran al alcance de empresas, Estados e incluso particulares[4].

Muchos de los resultados obtenidos con las herramientas de IA están relacionados con personas, lo que implica que dentro del gran conjunto de datos que se recogen mediante la técnica del *big data* o macrodatos se están recolectando datos de carácter personal. Lo anterior crea un riesgo para el titular si no se hace un tratamiento responsable, ético y transparente que proteja sus derechos y libertades. Esta situación que se presenta con gran facilidad en esta época en la que "el internet de las cosas"[5], la robótica y en general la tecnología están dominando al

3 Intel. The Rise in Computing Power: Why Ubiquitous Artificial Intelligence is Now a Reality. *Forbes.* [Citado el 20 de abril de 2019]. https://www.forbes.com/sites/intelai/2018/07/17/the-rise-in-computing-power-why-ubiquitous-artificial-intelligence-is-now-a-reality/#3b0120691d3f.

4 Garriga Domínguez, Ana. *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua* (Madrid: Dykinson, 2015).

5 Rose, Karen, Eldridge, Scott y Chapin, Lyman. *La internet de las cosas. Una breve reseña.* (Internet Society, 2015). El término internet de las cosas se refiere a escenarios en los que la conectividad de red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario que habitualmente no se consideran computadoras, permitiendo que estos dispositivos generen, intercambien y consuman datos con una mínima intervención humana.

mundo. Ese mismo lugar donde la interconexión digital y transmisión entre los diferentes dispositivos, objetos, personas y empresas se hace cada vez más rápido, en más territorios y con infinidad de actores.

LAS REGULACIONES SOBRE DATOS PERSONALES

En muchos países existen reglamentos y leyes sobre protección de datos personales, sin embargo, dichos marcos normativos, como en el caso colombiano, fueron diseñados en un momento en el que la cantidad de datos era limitada, se podía tener control sobre quiénes hacían su tratamiento y las finalidades para las cuales estaban siendo usados. El rápido avance de la tecnología y las herramientas de IA han traído cambios que posibilitan el procesamiento de millones de datos en diferentes partes del mundo y por diferentes actores a una velocidad inimaginable, estos cambios han provocado que las regulaciones se encuentren desactualizadas frente a estos nuevos retos.

En el caso de Colombia existe un vacío en relación con los actores involucrados en el tratamiento de los datos como los responsables, encargados y titulares, ya que no tienen parámetros definidos para actuar en esta nueva era de las tecnologías. Por tanto, si se quiere sacar beneficio de las posibilidades que ofrece la era digital, la IA y el *big data*, se deben establecer nuevas reglas, prácticas y garantías efectivas para la protección de los datos personales.

El Régimen de Protección de Datos Personales en Colombia se encuentra regulado por el artículo 15 de la Constitución Política, acompañado por dos leyes estatutarias: (i) la Ley 1266 de 2008, que regula el derecho a la protección de datos personales frente a información financiera, crediticia, comercial, de servicios y la proveniente de terceros países; y (ii) la Ley 1581 de 2012, que regula de manera general el tratamiento de datos personales, en la cual se establece la protección del derecho fundamental que tienen todas las personas a conocer, actualizar y rectificar sus datos personales[6] y a autorizar el tratamiento de la información que es almacenada en diferentes bases de datos bajo los principios de legalidad, finalidad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

En la citada normativa, no se contemplan disposiciones relacionadas con la era digital. Lo anterior implica que dentro de la actual regulación colombiana no se contempla el uso de las nuevas herramientas de IA mediante las cuales se recolectan datos, como *cookies*[7] y el *web crawling*[8], y las finalidades que se desarrollan por

6 Colombia. Congreso de la República. Ley Estatutaria 1581. *Por la cual se dictan disposiciones generales para la protección de datos personales* (Bogotá: 2012).

7 BBC News Mundo. Cómo borrar tu historial de navegación, búsqueda y descargas en internet. *BBC News Mundo.* [Citado el 20 de abril de 2019]. https://www.bbc.com/mundo/noticias-47443353.

8 Cambrige Dictionary. ¿Qué es un crawler o spider? *Cambridge Dictionary* [Citado el 20 de abril de 2019]. http://tejedoresdelweb.com/w/%C2%BFQu%C3%A9_es_un_crawler_o_spider%3F

medio de estas como: i) la creación de contenidos personalizados; ii) decisiones automatizadas y iii) *profiling* o generación de perfiles[9]. Sobre lo anterior, algunos autores de doctrina colombiana han indicado lo siguiente:

> La inexistente o deficiente regulación sobre temas propios de la era digital radica en la consecuente desprotección de los Titulares de los datos personales que sean tratados bajo esas nuevas dinámicas. Lo anterior, teniendo en cuenta el principio de legalidad según el cual, en el caso de los particulares, todo lo que no esté expresamente prohibido, está permitido. Siendo así, al no existir regulación alguna en la materia, se entiende que las fuentes de datos, tratamientos y finalidades que se han popularizado a raíz de la era digital se encuentran en principio permitidas y sin limitación alguna.[10]

Así mismo, otro de los vacíos con los que cuenta la legislación colombiana es que está limitada y es insuficiente en el ámbito de aplicación territorial para la era digital, ya que no contempla el tratamiento de los datos personales en medios ubicados fuera del país.

A diferencia del régimen colombiano, la Unión Europea ha trabajado en adaptar sus regulaciones a la era digital y la IA, adoptando en diferentes documentos directrices sobre estos temas. En primer lugar, está el Reglamento General de la Unión Europea de Protección de Datos Personales (RGDP), expedido el 25 de mayo de 2018, en el cual se establece en sus considerandos 6 y 7 que la rápida evolución y revolución tecnológica, que se ha realizado en poco tiempo, y la magnitud de la recolección y del intercambio de datos personales ha aumentado de manera significativa[11]. Es por esto que de acuerdo con el considerando 7 se ha llevado a la necesidad de crear un marco de datos personales más actualizado frente a la nueva era digital que permita desarrollar la economía aprovechando las nuevas tecnologías que esta era trae, como se muestra a continuación:

> Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales.

9 Cambrige Dictionary. Defición de Profiling. *Cambrige Dictionary.* [Citado el 20 de abril de 2019] https://dictionary.cambridge.org/es/diccionario/ingles/profiling. *Profiling* o generación de perfiles: práctica o método de seleccionar un conjunto de características pertenecientes a una determinada clase o grupo de personas o cosas por las cuales identificar individuos como pertenecientes a dicha clase o grupo.

10 Newman, Vivian y Ángel, María Paula. *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital* (Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2019).

11 El Parlamento Europeo y el Consejo de la Unión Europea. *Reglamento general de protección de datos.* Unión Europea: Consejo de la Unión Europea, 2016. Considerando n.º 6.

> Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades publicas.[12]

Así mismo, en el artículo 4, sobre definiciones, se presenta un listado actualizado de diferentes conceptos que están cada vez más presentes en el uso de las herramientas de IA y de la era de la tecnología como son: la inclusión dentro de los datos personales, los relacionados con la localización y los recolectados por identificadores en línea como las direcciones IP. Igualmente, se incluyeron las definiciones de elaboración de perfiles y la pseudonimización de los datos. La identificación y definición de estos conceptos han permitido aclarar aspectos que antes no se tenían en cuenta o no se entendían, con lo que se ha logrado un mejor conocimiento al momento de aplicar la nueva legislación.

En la mencionada legislación, en el artículo 22, se regulan también las decisiones automatizadas y la creación de perfiles. En este, se dispone que para la realización de este tipo de actividades será necesario: a) la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) el responsable debe establecer medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; c) el consentimiento debe ser explícito por parte del titular[13].

Es importante resaltar el artículo 3 de la RGPD sobre el ámbito territorial, ya que este señala que la normativa se aplicará también a los responsables de tratamiento de datos que, a pesar de no tener un establecimiento en Europa, dirijan sus ofertas de bienes o servicios a ciudadanos de la Unión Europea, o que controlen su comportamiento[14].

Finalmente, es pertinente traer al presente análisis lo establecido en el artículo 40 del RGDP, que promueve la elaboración de códigos de conducta[15] destinados a contribuir a la correcta aplicación del presente reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades de las micro, pequeñas y medianas empresas[16]. Lo anterior, es muy importante teniendo en cuenta que si las empresas empiezan a aplicar buenas prácticas, regulaciones y medidas de seguridad con base en un reglamento adaptado a la era de la tecnología, se beneficiarán y al mismo tiempo protegerán los intereses de los titulares.

Otro de los documentos que expidió la Unión Europea a través de la Comisión Europea en relación con la IA y las nuevas tecnologías fue "El Proyecto de Guía

12 Ibíd., considerando n.º 7.

13 Ibíd., artículo 22.

14 ARENAS RAMIRO, MÓNICA. *Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades. Hacia un nuevo derecho europeo de protección de datos* (Valencia: Tirant Lo Blanch, 2015).

15 VIGURI, JORGE. La implementación de nuevos esquemas de certificación en la UE como garantía de los derechos fundamentales de consumidores y usuarios. *Revista CESCO de Derecho de Consumo*, (2016): 28-40.

16 Op. cit. El Parlamento Europeo y el Consejo de la Unión Europea. Literal 1) artículo 40.

Ética para el Uso Responsable de la Inteligencia Artificial", en la cual, 52 expertos están participando en su elaboración centrándose en el ser humano siempre bajo la luz de la defensa de los derechos fundamentales, pues como explicó la comisaria europea de Economía y Sociedad Digitales, Mariya Gabriel, "El uso de la IA, como de cualquier tecnología debe estar siempre en línea con nuestros valores y defender los derechos fundamentales"[17]. El Proyecto de la Guía fue publicado el 18 de diciembre de 2018 para comentarios hasta el 1 de febrero de 2019. Algunos de los puntos que más se pueden destacar de la Guía son:

- Un enfoque de la IA centrado en los seres humanos.
- Garantizar el fin ético de la IA.
- La especial atención a los grupos vulnerables, como son los menores de edad o las personas con discapacidades.
- El respeto por los derechos fundamentales de los titulares.
- Los principios de transparencia, privacidad y seguridad de los datos personales.
- La importancia de la libertad humana[18].

Lo anterior muestra cómo varias prácticas, que se llevan a cabo en materia de protección de datos personales en otros países, no han sido contempladas por el régimen de datos personales que rige en Colombia. Lo que se pretende proponer con esta comparación no es que Colombia copie el modelo o documentos de la Unión Europea, sino que nuestro país lo utilice como guía para implementar los diferentes elementos contemplados en el RGPD y en la Guía Ética para el Uso Responsable de la IA, lo que permitirá construir normativas mucho más fuertes, claras, flexibles y actualizadas en el tratamiento de los datos de la era digital, teniendo en cuenta que los datos no solo se generan en un territorio, sino en todas partes del mundo y traspasan fácilmente los límites fronterizos gracias al internet y al comercio electrónico.

EL RIESGO DE LOS DATOS PERSONALES

Con el fin de resaltar la necesidad que existe en Colombia para la implementación de nuevas medidas de protección de datos personales relacionados con la Inteligencia Artificial (IA), es importante indicar que la disponibilidad del *big data* y el uso de las herramientas de la IA pueden generar riesgos para el titular de los datos. Entre otros, se encuentran la creación de perfiles —tanto exactos como inexactos—, robos, extorsiones, suplantación de identidad e inclusive usos para fines políticos ilegales. En este sentido, los nuevos escenarios tecnológicos y avances digitales han

17 *La Vanguardia*. Redacción. Bruselas ultima sus orientaciones éticas para la inteligencia artificial. *La Vanguardia.* [Citado el 20 de abril de 2019]. https://www.lavanguardia.com/politica/20181218/453636972739/bruselas-ultima-sus-orientaciones-eticas-para-la-inteligencia-artificial.html.

18 Ibíd.

demostrado que la protección de la vida privada y los datos personales pueden ser afectados de diversas formas e intensidades y que afectan no solo a un territorio, sino a titulares en varios países del mundo. Se incluyen así titulares ubicados en Colombia, ya que muchas de las plataformas y herramientas son usadas no solo en un territorio, sino en varios países a nivel mundial; por tanto, los riesgos y mal uso que suceden en un país pueden afectar la información de personas ubicadas en otro.

Así las cosas, los escándalos a nivel mundial que a continuación se mencionan, son una clara muestra de cómo un mal uso de datos por medio de herramientas de la IA puede causar un daño grave a los titulares de los datos no solo en un país, sino en varios países del mundo. En primer lugar, tenemos el caso de Cambridge Analytica, una empresa de análisis de datos políticos que de acuerdo con lo expuesto por el diario británico The Guardian, en colaboración con los periódicos The New York Times, usó sin autorización los datos personales de más de cincuenta millones de usuarios de Facebook[19], con el propósito de manipular psicológicamente a los votantes en las elecciones de Estados Unidos en el 2016, donde Donald Trump resultó electo presidente. La manera como se obtuvieron estos datos fue a través de un test de personalidad desarrollado por el profesor de la Universidad de Cambridge, Aleksandr Kogan. Dicho test fue completado por 265 000 usuarios, lo que estos no sabían, es que mediante el acceso al test estaban permitiendo que una aplicación de Facebook sustrajera datos como nombres, fechas de nacimiento, geolocalización, lista de las páginas a las que se les daba "me gusta"; además, esto no analizaba solo su perfil, sino el perfil de todos sus contactos, permitiendo realizar un *profiling* o generación de perfiles[20], el cual fue vendido a la empresa Cambridge Analytica y utilizada por esta para identificar cuál debía ser el contenido de los mensajes, los temas y las palabras a utilizar para cambiar la forma de pensar de los votantes y obtener el triunfo de Donald Trump[21]. En este caso, se demuestra cómo se hizo un tratamiento abusivo de los datos personales mediante una herramienta de captación de información sin que el titular lo supiera, afectando de esta manera la privacidad, el consentimiento y el derecho fundamental de la intimidad de los usuarios de Facebook.

A raíz del anterior escándalo, varios países del mundo —como Irlanda, Estados Unidos, Gran Bretaña, Francia, Países Bajos, Canadá, Australia y Nueva Zelanda— expidieron directrices de seguridad y buen tratamiento de los datos que debe cumplir Facebook para poder continuar funcionando. De manera similar, en Colombia, la Superintendencia de Industria y Comercio expidió la Resolución 1321 de 2019, por medio de la cual estableció que esta red social deberá adoptar nuevas medidas y mejorar las existentes para garantizar

19 *The Guardian*. Redacción. Facebook fined for data breaches in Cambridge Analytica scandal. *The Guardian*. [Citado el 20 de abril de 2019]. https://www.theguardian. com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scanda

20 Op. cit., Cambridge Dictionary.

21 Parlament UK. The issue of data targeting, based around the Facebook, GSR and Cambridge Analytica allegations. *Parliamentary business*. [Citado el 20 de abril de 2019].

la seguridad de los datos personales. Esto fue necesario teniendo en cuenta que, en el país, Facebook es la red social más usada, de acuerdo con la Primera Gran Encuesta TIC/2017 titulada "Estudio de acceso, uso y retos de las TIC en Colombia" realizada en el 2017 por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Otro de los casos, en el que se usó la IA para captar datos de forma ilegal, fue Joffe V. Google Inc.[22]. En este, se recolectaron datos personales a través de redes Wifi abiertas con los coches de su servicio Street View sin que los titulares supieran. En el 2007, Google lanzó su función Street View en Estados Unidos para complementar su servicio de Google Maps, al proporcionar a los usuarios fotografías panorámicas a nivel de la calle. Entre el 2007 y el 2010, Google también equipó sus autos Street View con antenas wifi y *software* que recopilaba datos básicos transmitidos por redes wifi en hogares y empresas cercanas como el nombre de la red (SSID), la intensidad de la señal, entre otros, con el supuesto fin de proporcionar servicios mejorados. No obstante, las antenas del *software* instalado en los autos de Street View de Google recolectaron más que solo la información de identificación básica transmitida por las redes wifi, también recopilaron y almacenaron todos los datos transmitidos por los dispositivos móviles conectado a redes wifi abiertas como correos electrónicos, nombres de usuario, contraseñas, videos, documentos personales y conversaciones telefónicas. En el 2010, Google reconoció que sus vehículos de Street View habían estado recolectando fragmentos de datos personales por medio de redes wifi sin cifrar y que esto había sucedido en más de treinta países a nivel mundial, por lo que varias demandas judiciales se presentaron poco después del anuncio de Google[23]. El anterior caso es un claro ejemplo de cómo el uso indebido del manejo de estos sistemas puso en riesgo la información, los derechos de los usuarios y, en general, a la sociedad, ya que no se tuvo conocimiento ni control sobre la recolección y uso de los datos de carácter personal ni por parte de los titulares ni de la misma empresa.

Los casos anteriores comprueban una falla en el sistema de protección de datos personales en diferentes países para el momento en que se realizaron los actos imputados en cada uno de los casos. Debe entonces tenerse en cuenta que el desarrollo de tecnologías relacionadas con IA probablemente seguirá teniendo un crecimiento exponencial. Así lo indicó para la *Revista Summa*, Andrea Mandelbaum, presidente de Mc Luhan Consulting, donde expresó que: "Para 2020, casi todos los productos de software a nuestro alrededor estarán 'revestidos' de IA"[24]. Así, pues, se requiere necesariamente un robustecimiento de las legislaciones y el sistema aplicable a la protección de datos personales con el fin de que este funcio-

22 Find Law. Joffe V. Google Inc. *Find Law.* [Citado el 20 de abril de 2019]. https://caselaw.findlaw.com/us-9th-circuit/1643851.html.

23 Ibíd.

24 *Revista Summa*. El futuro de la inteligencia artificial. *Revista Summa.* [Citado el 20 de abril de 2019]. http://revistasumma.com/futuro-la-inteligencia-artificial/.

ne, ya que hoy en día el uso del internet, las herramientas de IA y las diferentes plataformas no solo afecta y pone en riesgo los datos de los residentes de un país, sino de una gran cantidad de usuarios a nivel mundial.

RESPONSABLES DEL TRATAMIENTO DE LOS DATOS PERSONALES

Ahora bien, para que se logre un buen tratamiento de datos personales, no solo se debe imponer la carga a los gobiernos, sino también a aquellos que manejan los datos personales, pues, aunque existan mandatos legales si estos no son aplicados por quienes hacen el tratamiento, ya sea como responsables[25] y encargados[26] del tratamiento de los datos personales, el vacío y el riesgo en el uso de los datos seguirá latente. Muchas de las empresas que están utilizando herramientas de Inteligencia Artificial (IA) emplean datos personales de manera indiscriminada, sin informar a los titulares las finalidades del tratamiento con quiénes se están compartiendo los datos, qué canales pueden usar para acceder a los datos, dónde se tienen almacenados, haciendo que el titular pierda el control de sus datos y poniendo en riesgo sus derechos y libertades, así como los derechos de terceros que pueden verse involucrados en el tratamiento, más aún en esta época en la que "el internet de las cosas"[27], la robótica, la IA y, en general, la tecnología están dominando al mundo y la interconexión digital entre dispositivos, objetos, personas, empresas y territorios, donde participan infinidad de actores, recolectando datos y, en varios casos, sin que el titular tenga conocimiento.

En Colombia y en la Unión Europea es deber de todos aquellos que hacen tratamiento de datos personales cumplir con el Principio de Responsabilidad Demostrada o *Accountability*, que busca que los mandatos legales sobre el tratamiento de los datos personales sean una realidad verificable y redunden en beneficio de los derechos de las personas[28], lo cual se podrá lograr mediante la implementación de mecanismos y protocolos internos de seguridad y control para el manejo de los datos eficientes.

> El éxito de los mecanismos dependerá del compromiso real de todos los miembros de una organización, pero, especialmente, de los directivos de las organizaciones ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos.[29]

25 Op. cit. Colombia. Congreso de la República. Ley Estatutaria 1581. Literal e) artículo 3.

26 Op. cit. Colombia. Congreso de la República. Ley Estatutaria 1581. Literal d) artículo 3.

27 Op. cit. Rose, Karen, Eldridge, Scott y Chapin, Lyman.

28 Superintendencia de Industria y Comercio. Guía para la implementación del Principio de Responsabilidad Demostrada (*accountability*). *Superintendencia de Industria y Comercio.* [Citado el 20 de abril de 2019].

29 Colombia. Superintendencia de Industria y Comercio. Resolución 1321. *Por la cual se imparten órdenes dentro de una actuación administrativa* (Bogotá: Radicación 18233402 del 24 de enero de 2019).

Así mismo, es importante que además de acatar las directrices nacionales e internacionales establecidas por los diferentes entes gubernamentales, se implementen mecanismos de autorregulación para que las empresas determinen los parámetros de acuerdo con el tipo de organización, los datos tratados, el tipo de titulares, entre otros. La autorregulación es entendida como:

> La capacidad que tiene un sujeto, o una institución, organización o asociación, de regularse a sí misma bajo controles voluntarios. En los distintos ámbitos privados, la autorregulación se constituye como la potestad de establecer reglas por parte del cada sujeto dentro de su esfera de acción, estableciendo –de manera voluntaria y quizás espontánea normas deontológicas y códigos de autocontrol.[30]

Teniendo en cuenta lo anterior, es importante que los mecanismos que se establezcan estén siempre direccionados a la transparencia, la licitud, la libertad de decisión y la finalidad del tratamiento, lo que implica que cualquier acción que se realice sobre los datos personales debe ser lícita, informada de forma unívoca y que el titular debe dar su consentimiento expreso para el tratamiento. Sin embargo, como menciona la Red Iberoamericana de Protección de Datos (RIPD),

> La autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales.[31]

Uno de los mecanismos de autorregulación que puede ser implementado por los responsables del tratamiento es la protección de datos desde el diseño que consiste en que la privacidad se integre desde el inicio en la gestión y ciclo de vida del tratamiento de datos como se establece en el Considerando 78 del RGPD, a saber:

> Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al

30 Prosoft 2.0. Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI. *Prosoft 2.0.* [Citado el 20 de abril de 2019]. https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf, p.13

31 Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. *Red Iberoamericana de Protección de Datos.* [Citado el 20 de abril de 2019]. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/RIPD-AUTORREGULACI%C3%93N-Y-PROTECCI%C3%93N-DE-DATOS-PERSONALES-BOLIVIA-2006.pdf.

> estado de la técnica, de que los Responsables y los Encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.

Otro de los mecanismos de autorregulación que pueden ser utilizados por los responsables para la protección de los datos personales son la pseudonimización entendida como:

> El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identifica.[32]

O en la medida de lo posible, anonimización, lo cual tiene como finalidad:

> Eliminar o reducir al mínimo los riesgos de re identificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.[33]

Lo anterior con el fin de que los datos no estén ligados a una persona específica y puedan ser de una manera más segura y efectiva. De igual manera, la minimización en la recolección de los datos a los necesarios para el tipo de tratamiento, la limitación de las finalidades, los protocolos de seguridad, las políticas internas sobre el tratamiento de los datos y la capacitación al personal que maneja los datos, serán mecanismos de ayuda para la protección de estos. Estos mecanismos deben garantizar la privacidad, la seguridad y evaluar el impacto que puede tener el tratamiento de esos datos sobre los derechos y libertades de los titulares, siempre teniendo de presente que ya no se habla de un tratamiento de un pequeño grupo de datos, sino de datos masivos de carácter personal. Es indispensable que cuando se realice el tratamiento de los datos personales se obtenga un consentimiento libre e informado por parte del titular, en el que se establezcan las finalidades, los responsables y los tipos de tratamiento de una manera lo suficientemente comprensible para que pueda entender las razones detrás de la decisión de dar el consentimiento para el uso de sus datos.

Un ejemplo de los avances que algunas de las grandes empresas responsables han implementado fue la constitución, en el 2016, de la Asociación para la IA —la

32 Op. cit. El Parlamento Europeo y el Consejo de la Unión Europea. Numeral 5. Artículo 4.

33 Agencia Española de Protección de Datos. *Orientaciones y garantías en los procesos de anonimización de datos personales* (Madrid: Agencia Española de Protección de Datos, 2019).

Partnership on Artificial Inteligence— en beneficio de las personas y la sociedad con el fin de "estudiar y formular las mejores prácticas sobre las tecnologías de la IA", las empresas que hacen parte de esa asociación son Amazon, Apple, Google, Facebook, IBM y Microsoft. Así mismo, DeepMind, una de las compañías líderes mundial de IA, adquirida por Google en 2014, presentó un nuevo comité de ética "para ayudar a los tecnólogos a poner en práctica la ética y para ayudar a la sociedad a anticipar y dirigir el impacto de la IA de manera que trabaje para el beneficio de todos"[34].

Mediante la implementación de mecanismos por parte de los responsables de los datos personales, que estén enfocados en la protección de los derechos y libertades de los titulares, y en las regulaciones nacionales e internacionales, se podría lograr el equilibro de la protección de los derechos a la intimidad y la protección de datos personales con el desarrollo económico y la innovación, el uso de nuevas tecnologías para obtener un gran beneficio de la era digital y las herramientas de IA que ella trae. Sin embargo, se debe tener claro que, a pesar de los esfuerzos de los gobiernos y los responsables, el adecuado tratamiento dependerá también del papel que desempeñe el propio titular frente a la protección y cuidado de sus datos.

TITULARES DE LOS DATOS PERSONALES

Los titulares desempeñan un papel muy importante dentro del tratamiento de sus datos personales, pues no es solo responsabilidad de los terceros el buen uso de los datos sino de los mismos titulares, ya que muchas veces son ellos mismos quienes entregan sus datos desmedidamente sin tener conciencia ni conocimiento de las implicaciones que esto puede generar. Un ejemplo de esto son los titulares de datos personales, que mediante internet se suscriben crecientemente a diversos sitios como:

> Redes sociales, plataformas audiovisuales o de mensajería instantánea como Gmail, Facebook, Instagram, Outlook, Netflix, WhatsApp o YouTube, ¡¡¡a navegadores web como Google, Bing o Yahoo!!!!, a tiendas online tipo Amazon, EBay, Dafiti o Mercado Libre, a medios de comunicación con plataformas virtuales como El Espectador, The New York Times, El Tiempo, The Guardian, Las 2 Orillas, Semana, Times, entre otros.[35]

Estos sitios de Internet recolectan un sin número de datos sin control y sin saber quiénes hacen tratamiento de sus datos y dónde se están almacenando. Así mismo,

34 Barrios, Moisés. *El País*. Redacción. *¿Deben los Estados regular la inteligencia artificial?* [Citado el 20 de abril de 2019]. https://retina.elpais.com/retina/2018/09/25/tendencias/1537869431_203848.html

35 Romero, Graciela. Publicidad basada en el comportamiento en internet experiencia de la autoridad de protección de datos de Uruguay. *Redipd.* [Citado el 20 de abril de 2019]. http://www.redipd.es/actividades/encuentros/xi/common/Ponencias/P5_uruguay_texto.pdf.

los datos están siendo recolectados por medio de Cookies[36] y otras tecnologías de rastreo que la mayoría de las páginas de internet y aplicaciones usan para recolectar datos como el buscador y el tipo de dispositivo, lenguaje, tiempos de acceso, páginas visitadas, su dirección IP y las URL, datos y transacciones que la mayoría de titulares desconocen.

Los titulares usualmente no realizan un ejercicio juicioso de leer los términos y condiciones del uso de las herramientas, las políticas de tratamiento de información de datos personales desconocen y no ejercen sus derechos; esto produce la entrega de toda clase de datos, incluyendo datos privados y sensibles, datos que son usados por los responsables para realizar diferentes usos que pueden poner en riesgo la privacidad y los intereses del titular, como sucedió mediante las herramientas de analítica y la publicidad comportamental usadas en el caso de Cambridge Analytica, antes mencionado, en el que se logró identificar las preferencias, gustos y pasiones de los usuarios de Facebook para, de esta manera, ajustar el contenido[37] que veían los usuarios y obtener el objetivo que la compañía quería, es decir, el voto por el candidato Donald Trump, por medio de una manipulación de la mente del usuario, sin que este lo supiera.

Lo descrito trae como lección que el titular del dato debe ser más consiente y tener en consideración de las diferentes consecuencias y riesgos que pueden correr frente a sus datos personales y la privacidad de los estos, sino se ejerce un mayor control al momento de la entrega y la revisión de las finalidades para los cuales van a ser tratados. Así mismo, los usuarios pueden implementar algunas medidas sencillas para proteger sus datos personales como son: i) limitar los datos que se publican, no se debe compartir datos como dirección, datos personales, bancarios, números telefónicos o domicilios, ii) uso limitado de mensajes privados, es decir, no compartir contraseñas, datos bancarios y ninguna información comprometedora, ya que dichos mensajes además de captar información pueden ser objeto de *phishing*[38]; iii) borrar el historial de búsqueda del navegador, iv) utilizar la navegación incógnita para que herramientas como las *cookies* no puedan identificar a la persona; v) uso de contraseñas seguras, vi) uso de redes de wifi privadas, vii) leer los términos y condiciones de las plataformas y redes sociales a las que se adhieren.

La IA y la era digital no dan espera, razón por la cual se necesitan titulares preparados para afrontar los desafíos que estas traen, es decir, titulares digitales

36 Op. cit. BBC News Mundo.

37 SEAMANS, ROBERT. Artificial Intelligence and Big Data: Good for Innovation? *Experience Faculty & Research.* [Citado el 20 de abril de 2019]. https://www.stern.nyu.edu/experience-stern/faculty-research/artificial-intelligence-and-big-data-good-innovation.

38 Alegsa. Definición de Phishing. *Diccionario de informática y tecnología* [Citado el 20 de abril de 2019]. http://www.alegsa.com.ar/Dic/phishing.php. La palabra es un neologismo creado como un homófono de "pescar" en inglés (*fishing*) debido a la similitud de usar un cebo en un intento de atrapar a una víctima. El *phishing* es un intento fraudulento de obtener información delicada, como nombres de usuario, contraseñas y detalles de tarjetas de crédito (y dinero), a menudo por razones maliciosas, disfrazándose como una entidad confiable en una comunicación electrónica (un *email*, un SMS, o cualquier otro mensaje). Diccionario de Informática y Tecnología. Alegsa.

adaptados al siglo XXI, conocedores de los riesgos, las garantías y las facultades que le pertenecen; titulares empoderados de la protección de sus datos y el cumplimiento de sus derechos. Este proceso debe empezar desde los colegios y universidades, para que, a partir de una etapa temprana, puedan como ciudadanos y desarrolladores de nuevas herramientas tecnológicas tener una visión ética y responsable en el uso de los datos personales y la IA.

CONCLUSIONES

Actualmente son pocas las áreas en las que no se aplica la IA o algún tipo de herramienta tecnológica, cada día son más personas las que hacen uso de nuevos servicios y dispositivos tecnológicos, por tanto, cada día se crean y almacenan más datos en la red[39]. La era digital, la IA y el *big data* es un hecho con el que debemos aprender a vivir. Sin embargo, se requiere reflexionar sobre el papel que desempeñan las normas, leyes y regulación, el valor que los titulares dan a sus derechos en cuanto a la protección de datos personales, su privacidad y el tratamiento que se dará a los datos personales. Deben existir reglas claras entre todos los actores, pues cualquiera de las partes puede afectar la cadena de protección de la información.

Es fundamental que los gobiernos y las instituciones (locales, regionales, nacionales, internacionales) estén al tanto de los avances y agilicen los trámites necesarios para la expedición de nuevas regulaciones adaptadas a la era digital, pues la falta de regulación crea vacíos en cuanto a las prácticas que se pueden realizar mediante la IA, los límites del uso de los datos personales, las medidas de seguridad y las sanciones por un mal uso de los datos personales, ya que uno de los problemas actuales es que las normas de protección de estos datos no avanzan al mismo ritmo de las nuevas tecnologías, provocando que las regulaciones sean precarias en cuanto a la realidad actual.

Como punto de partida y ejemplo para las diferentes regulaciones, incluyendo la colombiana, existe el Reglamento Europeo de Protección de Datos Personales, el cual fue elaborado con base en el desarrollo de la era digital y las nuevas tecnologías, permitiendo la protección de los derechos de los titulares de los datos personales, pero sin frenar el desarrollo de las nuevas tecnologías. Así mismo, no solo deben existir reglamentos sobre protección de datos personales, sino documentos que manejen directrices específicas sobre diferentes temas como, por ejemplo, la Guía Ética para el Uso Responsable de la Inteligencia Artificial, Guía para la Implementación del Principio de Responsabilidad Demostrada (*accountability*), entre otros. Dichos documentos complementan y dirigen a todos los actores involucrados en los diferentes tratamientos, orientándolos a realizar prácticas adecuadas para proteger

39 Agencia Española de Protección de Datos Personales. 25 años de la Agencia Española de Protección de Datos - Acompañando al Ciudadano en su transformación Digital. *Agencia Española de Protección de Datos Personales*. [Citado el 20 de abril de 2019]. https://www.aepd.es/media/estudios/25-aniversario-AEPD.pdf.

los derechos de los titulares y los intereses de la misma sociedad. Sin embargo, cabe destacar que todas las políticas, directrices y regulaciones deben ser enfocadas bajo los principios de privacidad, responsabilidad y transparencia para generar seguridad y confianza en el tratamiento de los datos y bajo el contexto de cada territorio.

Como se ha mencionado en el presente documento, la protección de los datos personales no solo es una responsabilidad de los gobiernos, los responsables del tratamiento son la piedra angular en la protección de los derechos de los titulares, ya que son ellos quienes están haciendo el uso masivo de los datos (*big data*) para que el funcionamiento de todas sus herramientas de IA. Por tanto, sus buenas prácticas, la transparencia que ellos tengan frente a los titulares, así como la privacidad y la seguridad con las que manejen los datos son factores clave para generar la confianza de los titulares y así incentivar el uso de las nuevas tecnologías y promover el desarrollo de la sociedad, pero bajo un esquema de responsabilidad, conciencia y protección, pues como señaló el vicepresidente para la Agenda Digital del Ejecutivo Comunitario, Andrus Ansip, "para que la gente acepte y utilice sistemas basados en inteligencia artificial necesita confiar en ellos, saber que su privacidad es respetada, que las decisiones no son parciales", solo aquellas empresas que estén preparadas para abrazar estas tecnologías lograrán crear negocios sostenibles en el tiempo y ser sobre todo competitivos.

Sin embargo, para que funcionen los esfuerzos realizados por los gobiernos y los responsables del tratamiento de los datos, es imprescindible un mayor involucramiento de la ciudadanía frente al conocimiento de sus derechos como titulares de los datos personales, ya que muchas veces ni siquiera saben que los tienen, deben estar más atentos a las tecnologías que usan y consultan, así como a los tipos de datos que están aportando. Así mismo, también deberá existir la provisión de recursos de parte del Estado y el planteamiento de estrategias más amplias de divulgación para dotar los ciudadanos de las herramientas suficientes que les permite entender las implicaciones que tiene esta era digital, siendo cada persona veedora de sus derechos y estando preparados para responder a los riesgos que se va a enfrentar el tratamiento de sus datos.

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PERSONALES. 25 años de la Agencia Española de Protección de Datos - acompañando al ciudadano en su transformación digital. Agencia Española de Protección de Datos Personales. 2018. [Citado el 20 de abril de 2019.] https://www.aepd.es/media/estudios/25-aniversario-aepd.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Orientaciones y garantías en los procesos de anonimización de datos personales*. Madrid: Agencia Española de Protección de Datos, 2019.

ALEGSA. *Definición de phishing. Diccionario de informática y tecnología*. 2009. [Citado el: 20 de abril de 2019.] http://www.alegsa.com.ar/Dic/phishing.php.

Arenas Ramiro, Mónica. *Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades. Hacia un nuevo Derecho europeo de protección de datos*. Valencia: Tirant Lo Blanch, 015.

BBC News Mundo. Cómo borrar tu historial de navegación, búsqueda y descargas en internet. *BBC News Mundo*. [Citado el 20 de abril de 2019]. https://www.bbc.com/mundo/noticias-47443353.

Barrios. Moisés. *El País.* Redacción. ¿Deben los Estados regular la inteligencia artificial? [Citado el 20 de abril de 2019]. https://retina.elpais.com/retina/2018/09/25/tendencias/1537869431_203848.html

Cambridge Dictionary. ¿Qué es un crawler o spider? Cambridge Dictionary. [Citado el 20 de abril de 2019]. http://tejedoresdelweb.com/w/%C2%BFQu%C3%A9_es_un_crawler_o_spider%3F

Cambridge Dictionary. Definición de Profiling. Cambridge Dictionary. [Citado el 20 de abril de 2019] https://dictionary.cambridge.org/es/diccionario/ingles/profiling.

Colombia. Congreso de la República. Ley Estatutaria 1581. Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: 2012.

Colombia. Superintendencia de Industria y Comercio. Resolución 1321. Por la cual se imparten órdenes dentro de una actuación administrativa. Bogotá: Radicación 18233402 del 24 de enero de 2019.

El Parlamento Europeo y el Consejo de la Unión Europea. *Reglamento general de protección de datos*. Unión Europea: Consejo de la Unión Europea, 2016.

Find Law. Joffe V. Google Inc. Find Law. 10 de septiembre de 2013. [Citado el 20 de abril de 2019] https://caselaw.findlaw.com/us-9th-circuit/1643851.html.

Garriga Domínguez, Ana. Nuevos retos para la protección de datos personales. En *la Era del Big Data y de la computación ubicua*. Madrid: Dykinson, 2015.

intel. The Rise in Computing Power: Why Ubiquitous Artificial Intelligence Is Now A Reality. Forbes. [Citado el 20 de abril de 2019] https://www.forbes.com/sites/intelai/2018/07/17/the-rise-in-computing-power-why-ubiquitous-artificial-intelligence-is-now-a-reality/#3b0120691d3f.

La Vanguardia. Redacción. Bruselas ultima sus orientaciones éticas para la inteligencia artificial. La Vanguardia. [Citado el 20 de abril de 2019]. https://www.lavanguardia.com/politica/20181218/453636972739/bruselas-ultima-sus-orientaciones-eticas-para-la-inteligencia-artificial.html.

Mayer-Schönberger, Viktor y Cukier, Kenneth. *Big Data. A Revolution That Will Transform How We Live, Work, and Think*. Madrid: Houghton Mifflin Harcourt, 2013.

Newman, Vivian y Ángel, María Paula. *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*. Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2019.

PARLAMENT UK. The issue of data targeting, based around the Facebook, GSR and Cambridge Analytica allegations. Parliamentary business. [Citado el 20 de abril de 2019]. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36306.htm.

PROSOFT 2.0. Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI. Prosoft 2.0. [Citado el 20 de abril de 2019]. https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf.

REAL ACADEMIA ESPAÑOLA. Definición inteligencia artificial. Real Academia Española. [Citado el 20 de abril de 2019] https://dle.rae.es/?id=LqtyoaQ.

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Red Iberoamericana de Protección de Datos. [Citado el 20 de abril de 2019]. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/RIPD-AUTORREGULACI%C3%93N-Y-PROTECCI%C3%93N-DE-DATOS-PERSONALES-BOLIVIA-2006.pdf.

REVISTA SUMMA. El futuro de la inteligencia artificial. Revista Summa. [Citado el 20 de abril de 2019] http://revistasumma.com/futuro-la-inteligencia-artificial/

ROMERO, GRACIELA. Publicidad basada en el comportamiento en internet experiencia de la autoridad de protección de datos de Uruguay. Redipd. [Citado el 20 de abril de 2019]. http://www.redipd.es/actividades/encuentros/XI/common/Ponencias/P5_URUGUAY_TEXTO.pdf.

ROSE, KAREN, ELDRIDGE, SCOTT Y CHAPIN, LYMAN. *La internet de las cosas. Una breve reseña*. Internet Society, 2015.

SEAMANS, ROBERT. Artificial Intelligence and Big Data: Good for Innovation? Experience Faculty & Research. [Citado el 20 de abril de 2019]. https://www.stern.nyu.edu/experience-stern/faculty-research/artificial-intelligence-and-big-data-good-innovation.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Guía para implementación del Principio de Responsabilidad Demostrada (*accountability*). Superintendencia de Industria y Comercio. [Citado el 20 de abril de 2019]. https://issuu.com/quioscosic/docs/guia_accountability_26_p__g.

VIGURI, JORGE. La implementación de nuevos esquemas de certificación en la UE como garantía de los derechos fundamentales de consumidores y usuarios. *Revista CESCO de Derecho de Consumo*, (2016): 28-40.

THE GUARDIAN. Redacción. Facebook fined for data breaches in Cambridge Analytica scandal. The Guardian. [Citado el 20 de abril de 2019]. https://www.theguardian. com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scanda