# RETOS PARA LA REGULACIÓN DEL BIG DATA Y LA INTELIGENCIA ARTIFICIAL: PRIVACIDAD, DEMOCRACIA Y DERECHOS HUMANOS

**TRABAJO DE GRADO**

**ANA MARÍA TRUJILLO**

**ASESOR**
**ANTONIO BARBOZA VERGARA**

**UNIVERSIDAD EAFIT**

**ESCUELA DE DERECHO**

**MEDELLÍN**

**2020**

# INTRODUCCIÓN

Los algoritmos de *big data* e inteligencia artificial dejaron de ser tecnologías cuya aplicación parecía distante para convertirse en herramientas esenciales en la sociedad contemporánea. A medida que avanzan estas tecnologías delegamos cada vez más decisiones en cabeza de estos algoritmos, mientras que cedemos nuestra autonomía. En el día a día, nos indican constantemente qué leer, qué mirar, qué escuchar en redes sociales, aplicaciones, plataformas, buscadores, etc sin ser cuestionados. En los mercados, permiten identificar necesidades y comportamientos de los consumidores, reducir tiempos en los procesos productivos, aumentar la productividad, facilitar el acceso y distribución de bienes y servicios, y generar así aumentos significativos en los ingresos (Martínez, 2018, p. 6). En general, en cualquier sector, el uso de algoritmos de b*ig data* e inteligencia artificial garantiza hacer más efectiva la toma de decisiones.

Las ventajas de aplicación de algoritmos en políticas de salud pública se han hecho evidentes en las últimas semanas para controlar la propagación del Covid-19. El *big data* ha marcado la diferencia entre países asiáticos y el resto del mundo: países como Italia, España, Alemania, superaron la barrera de los miles desde principios de marzo del presente año. En cambio, en países como China, Corea del Sur y Japón ya se superó la peor fase de infección del virus, y en Taiwán y Singapur no se han registrado más de 300 casos a pesar de su cercanía con china. La vigilancia digital, práctica arraigada en los países mencionados, ha permitido hacer valoraciones exhaustivas de la salud de los ciudadanos (Han, 2020).

En China, por ejemplo, todos los aspectos de la vida cotidiana están controlados y sometidos a observación, lo cual ha demostrado ser eficaz para contener la pandemia, pues cámaras de detección facial y sensores de temperatura permiten identificar a aquellos con temperaturas sospechosamente altas, a quienes se les impone estar en cuarentena. Asimismo, el sistema notifica a las personas con las que el posible enfermo tuvo contacto y verifica el cumplimiento de las medidas de cuarentena a través de drones. Pero por más eficaces que sean estas medidas, el precio a pagar en términos de derechos humanos es alto. La recopilación de los datos que alimentan los algoritmos y les permiten tomar decisiones

implica que cada aspecto de la vida se somete a vigilancia, no existe protección a los datos personales ni a la esfera privada, ni la posibilidad de controvertir el régimen (Han, 2020).

El uso de algoritmos en la lucha contra el coronavirus evidencia la idea principal de este trabajo: las decisiones basadas en datos son la manera más efectiva de lograr un fin, pero su uso desmedido y sin límites trae como consecuencia la potencial afectación a un repertorio de derechos humanos y valores esenciales para las sociedades actuales. Por tal motivo, es necesario un marco normativo que permita conciliar la necesidad de progreso y que garantice que las decisiones automatizadas no son contrarias a los derechos humanos.

Para tal fin, en el primer capítulo del presente trabajo se realizará una descripción teórica de las tecnologías objeto de estudio, esto es, el big data y la inteligencia artificial. En el segundo capítulo se expondrán distintos casos en los que algoritmos de b*ig data* e inteligencia artificial, así como la ingeniería de datos, han sido las herramientas esenciales en la realización de planes de vigilancia masiva, en la creación de publicidad cognitiva dirigida al elector, y en la manipulación a la opinión pública. En línea con lo anterior, en el tercer capítulo, se realizará un análisis teórico y conceptual a partir de el Reglamento General de Protección de Datos Personales de la Unión Europea (RGDP) y los recientes trabajo de autores como Kate Crawford & Jason Schultz (2014), Lorenzo Cotino Hueso (2017), Maria Paula Ángel y Vivian Newman (2019), etc., sobre los posibles riesgos de la aplicación de estas tecnologías para para la privacidad y las normas de protección de datos personales. También se expondrán los potenciales riesgos que se derivan de las características propias de los algoritmos para la igualdad, la autonomía y la democracia, con base en los trabajos de Mireille Hildebrandt (2008), Lorenzo Cotino Hueso (20017, Luis González de la Garza (2018), Jimmy Waldron (2012) y Robert B. Talisse (2012).

Por último, en el cuarto capítulo se desarrollará un análisis jurídico en el que se examinará por qué es necesaria una aproximación internacional a la problemática de protección de datos personales y la regulación del uso de algoritmos. En este capítulo también se hará un recuento de las falencias del Régimen colombiano de protección de datos personales, compuesto por la Ley estatutaria 1581 de 2012, su respectivo decreto reglamentario y la sentencia C-748 de 2011, para afrontar las problemáticas en torno a la privacidad y al uso de

algoritmos, y la manera en que organismos de cooperación internacional han abordado estas problemáticas, como la Unión Europea a partir del RGDP y el Libro Blanco sobre Inteligencia Artificial y la Organización para la Cooperación y el Desarrollo Económico a partir de los principios promulgados en la Recomendación del Consejo de la OCDE sobre Inteligencia Artificial.

En ese orden de ideas, el presente trabajo permite concluir que el análisis de datos a partir del big data y la inteligencia artificial puede conllevar a la materialización de riesgos para la privacidad, la autonomía, la no discriminación y la democracia. Los riesgos para la privacidad están relacionados con el tratamiento indebido de datos personales y aquellos relativos a la autonomía, discriminación y democracia pueden presentarse como consecuencia de características propias de los algoritmos, como la falta de transparencia, es decir, el desconocimiento sobre la manera en la que el algoritmo toma decisiones. En consecuencia, el uso de algoritmos por actores estatales y no estatales en escenarios que comprometen los valores y principios democráticos manifiestan la necesidad de establecer un marco regulatorio de las tecnologías de procesamiento de la información desde la protección de datos personales y desde la regulación de los problemas que se derivan de su diseño

# 1. NUEVAS TECNOLOGÍAS PARA EL PROCESAMIENTO DE DATOS

Los algoritmos electrónicos y la minería de datos han cambiado la forma en que se procesan los datos y se toman decisiones. Gracias a las nuevas tecnologías de procesamiento de datos es posible analizar y extraer información de millones de datos en segundos. Bajo esta premisa, los datos han adquirido una importancia fundamental para las ciencias exactas, la sociedad, el mercado e, incluso, los Estados. A continuación, se explicará cuáles son esas nuevas tecnologías de procesamiento de datos que han permitido que el flujo de datos sea más eficiente, es decir, el *big data* y la inteligencia artificial. Posteriormente, se detallará qué es la minería de datos, así como los tipos de datos que son objeto de procesamiento y, por último, se expondrán algunos ejemplos de los distinto usos de estas herramientas.

## *1.1 Big data*

En primer lugar, el concepto de dato es definido por la Real Academia de la Lengua Española como la información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. Esta definición es imprecisa debido a que los datos no dicen nada por sí solos, para extraer conocimiento o deducir consecuencias de estos es necesario someterlos a procesamiento, esto es, recolectarlos, organizarlos y analizarlos para extraer información relevante sobre estos. En otras palabras, los datos no tienen un valor intrínseco, pues el valor está determinado por su procesamiento. Este último ha adquirido especial importancia en la última década a causa del aumento en la generación de datos, el cuial tiene su raíz en tres factores principales: el incremento de dispositivos con conexión a internet, el auge de las redes sociales y el internet de las cosas. (Casas, Nin & López, 2019, p. 24).

Existen dos formas en las que se ha procesado la información. Antes de la invención del internet en los años setentas, la información era procesada por sistemas informáticos de forma *autónoma*, es decir, sin que dicho sistema estuviese conectado a otros. La invención del internet permitió conectar varios sistemas informáticos, dando lugar al procesamiento *distribuido*. La conexión entre varios ordenares constituye el antecedente del análisis de datos

masivos ya que posibilitó analizar cantidades mayores de datos con mayor potencia y rapidez, lo cual sentó el precedente para la creación del *big data (*González, 2018, p. 275).

Se habló por primera vez del término *big data* en el ámbito de las ciencias exactas, especialmente en el campo de la astronomía y la genética, donde los avances científicos generaron más datos de los que se había acumulado alguna vez en la historia de estas ciencias. En un primer momento, la cantidad masiva de datos no solo llevó a los científicos a comprender que sus métodos de análisis eran arcaicos y que no podrían enfrentarse a su crecimiento exponencial, sino que constituyó un cambio de paradigma para las ciencias y, en general, para cualquier área del conocimiento que requiriera el análisis de datos.

Anteriormente, para analizar cualquier fenómeno era necesario recolectar muestras aleatorias de este y organizar los datos estructuradamente[1] para crear una hipótesis y establecer cuál sería la probabilidad de que las muestras y la hipótesis fuesen válidas. En lugar de muestras de datos recolectados cautelosamente, hoy en día es posible recolectar cantidades masivas de datos sin metodología alguna, es decir, de forma desestructurada. En la actualidad, los métodos de análisis estadístico suelen ser aplicables a conjuntos pequeños de datos estructurados, pero estas técnicas no son útiles para el análisis de datos masivos y desestructurados. Para el procesamiento de estos últimos, son necesarios algoritmos[2] que exceden con creces la capacidad del cerebro humano (Casas *et al*, 2019, p. 26-27; Holmes, 2017, p. 14- 16).

En ese sentido, el término se utiliza para referirse a la basta cantidad de datos generados y recogidos en bases de datos cuya extensión y complejidad requieren nuevos algoritmos para extraer información útil. Pero *big data* no se refiere únicamente a la magnitud de datos pues no se puede dejar de considerar la complejidad de los mismos, por lo cual se ha delimitado

[1] Un conjunto de datos se considera estructurado cuando es homogéneo, es decir, se organizan los datos según su tipología y todos tienen un denominador común, como una hoja de Excel. En cambio, los datos desestructurados son aquellos que combinan diferentes tipos de datos y no necesariamente guardan relación unos con otros, por ejemplo, una base de datos que contiene mensajes de texto, fotografías y videos.

[2] Un algoritmo es un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema (*Real Academia Española*, Citado el 11 de abril de 2020. Recuperado dehttps://dle.rae.es/algor%C3%Adtmico).

el término a partir de sus cuatro características principales, esto es, volumen, velocidad, variedad y veracidad (Holmes, 2017, p. 15-16), las cuales se explican a continuación:

A. Volumen

Este aspecto hace referencia a la cantidad de datos disponibles en la actualidad que hace imposible que puedan ser procesados por métodos estadísticos tradicionales con eficacia (Holmes, 2017, p. 16). De acuerdo con Luis González (2018), solo en Facebook se generan diariamente 10.000 millones de mensajes, se comparten 350 millones de fotografías y videos y se señalan con el ícono «me gusta» 4.500 millones de páginas, todos estos datos se almacenan en miles de servidores distribuidos a lo largo del mundo entero y son las fuentes de almacenamiento de la información de las que el *Big Data* extrae sus análisis predictivo en tiempo real (pp. 275-276)[3].

B. Velocidad

Se refiere a la rapidez con la que se generan nuevos datos en el día a día y a la celeridad con la que son procesados, razón por la cual este aspecto guarda una relación directamente proporcional con el volumen. (Holmes, 2017, p. 18). Para Jordi Casas *et al* (2019), este factor es fundamental porque si bien hay datos que se podrán analizar en días a partir de métodos tradicionales, en el campo del *big data* la velocidad es esencial y evidencia la necesidad de procesarlos en tiempo real dado el crecimiento exponencial de los datos (p. 29-31).

C. Variedad

Se refiere a las distintas fuentes de obtención de datos y a los formatos y estructuras en que estos se pueden presentar, es decir, de forma estructurada o desestructurada. El *big data* permite el procesamiento de ambos tipos de datos, siendo más frecuente el procesamiento de

[3] Este volumen de datos suele expresarse en *zettabytes* (ZB = 1,000,000,000,000,000 de bytes.). En otras palabras, si un *byte* equivale una letra y un *kilobyte* (KB= 1.000 bytes), a una historia muy corta, un *zettabyte* equivaldría a la colección impresa de la Biblioteca del Congreso de los Estados Unidos (Moleón-Getino, 2015, p. 430).

datos desestructurados, que incluirían conversaciones, fotos, geolocalización, tuits, videos, etc. (González, 2018, p. 276).

D. Veracidad

La veracidad se refiere a la calidad de los datos que son recolectados. Dependiendo de los tipos de datos que se analicen, la veracidad del análisis varía, como es el caso de los datos generados en redes sociales, que por naturaleza son imprecisos, inciertos o falsos. Por ejemplo, las publicaciones en redes sociales, conversaciones, registros telefónicos pueden contener errores gramaticales, ortográficos o palabras coloquiales que incidan en el resultado de este análisis, razón por la cual siempre habrá un margen de error (Casas *et al,* 2019, p. 26-27; Holmes, 2017, p. 18).

Si bien estos 4 elementos han sido comúnmente usados a la hora de describir el *big data,* es importante considerar que no hay consenso sobre su definición. Autores como Casas et al (2019), lo han descrito como "el conjunto de estrategias, tecnologías y sistemas para el almacenamiento, procesamiento, análisis y visualización de conjuntos de datos complejos, que dada su magnitud no pueden ser procesados por métodos tradicionales" (p. 45), pues estos autores consideran que su definición no se agota con describir las características de los datos que procesa. En definitiva, *big data* es un término generalizado e impreciso que puede referirse tanto a bases de datos masivos como al uso de metodologías de minería de datos y análisis predictivos (Crawford y Schultz, 2014, p. 96)

## *1.2 Inteligencia artificial (IA)*

Es de suma importancia resaltar que no existe consenso en la comunidad científica sobre las definiciones de *big data* e inteligencia artificial, razón por la cuál la distinción entre un concepto y otro suele ser difusa. La inteligencia artificial es entendida como la simulación de procesos o actividades humanas llevadas a cabo por máquinas dotadas con la capacidad de razonar, planificar y aprender (Martínez, 2019, p.7).

La aplicación de la inteligencia artificial más común es el aprendizaje automático o *machine learning*, herramienta definida por Casas et al (2019) como "el conjunto de métodos y algoritmos que permiten a una máquina aprender de manera automática con base en experiencias pasadas". En ese orden de ideas, estos autores describen la relación entre *big data* e inteligencia artificial de la siguiente forma: los métodos y algoritmos utilizados en el aprendizaje automático son los mismos que se utilizan en el *big data*, solo que este último siempre implicará el uso de volúmenes masivos de datos, razón por la cual los métodos pueden ser más complejos. Es decir, no todos los métodos y algoritmos de aprendizaje automático podrán ser empleados en el ámbito de los datos masivos, pero los datos masivos siempre implicarán métodos y algoritmos de aprendizaje automático (p. 61).

Por lo tanto, para efectos de este trabajo, cuando se habla de *big data* se hace referencia al uso de datos de volumen masivo y, de inteligencia artificial, cuando el volumen de los datos no es masivo.

### *1.3 Minería de datos*

Es común escuchar frases como "los datos son el nuevo petróleo" ya que, como el petróleo, los datos primero deben ser sometidos a un proceso para encontrar su valor. En ese sentido, la minería de datos no es más que la tarea de extraer información valiosa de bases de datos de volumen masivo. En otras palabras, se define como aquella rama de la informática y la estadística que, sirviéndose del *big data* o la inteligencia artificial, busca explorar y explotar datos, generalmente masivos, de manera automática o semiautomática, con el objetivo de encontrar patrones repetitivos que expliquen el comportamiento de estos datos. (Holmes, 2017, p. 20; Guevara, Medina y Vallejo, 2018, p. 377).

Un proyecto de minería de datos que usa el big data o la inteligencia artificial se desenvuelve en 4 fases: la primera consiste en la captura los datos de forma directa (recolección directa) o a partir de un mercado secundario (compraventa de bases de datos) y se pre-procesan, es decir, se corrige el formato de los datos. La segunda versa sobre el almacenamiento de los datos para facilitar su posterior consulta. La tercera consiste en el análisis de los datos, donde se aplican los algoritmos de aprendizaje automático para obtener los resultados deseados, ya sea predecir patrones, extraer conocimiento, establecer correlaciones, etc. Es decir, el

algoritmo puede desarrollar reglas para clasificar nueva información en categorías preexistentes o no usar ninguna regla con la finalidad de encontrar patrones escondidos o correlaciones distantes. Y, por último, una cuarta fase que consiste en la retroalimentación del modelo, es decir, confrontar los resultados con la realidad, para corregir o determinar la capacidad predictiva del modelo (Casas *et al*, 2018, p. 71; Holmes, 2017, p. 20).

### *1.4 Datos personales y datos de trafico*

Tanto el *big data* como la inteligencia artificial son utilizados con la finalidad de realizar análisis sobre conjuntos de datos cuyos resultados permiten individualizar al sujeto titular de esos datos, razón por la cual los datos que se usan son principalmente datos personales, pero no son los únicos. Hecha esta precisión, es importante distinguir dos categorías: datos personales y metadatos o datos de tráfico.

Los datos personales son aquellos que identifican un individuo en específico, es decir, que son atribuibles a una persona y permiten individualizarla. Son ejemplos de datos personales: los relacionados a los atributos de la personalidad como el nombre, el estado civil, nacionalidad, fecha y lugar de nacimiento; información biométrica como huellas, rostro; información morfológica como el color de la piel, estatura, peso; antecedentes personales de salud; pertenencia a grupos de promoción de derechos humanos, sindicatos, oenegés; ideología, orientación o identidad sexual, origen étnico, estrato socioeconómico, hisotrial crediticio, etc.

Los datos de tráfico o metadatos son “toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación y/o interoperabilidad” (Senso y Piñero, 2003, p. 99). En otras palabras, son datos que hablan de otros datos. Son ejemplos de estos: las direcciones IP, direcciones de email de remitente y destinatario al mandar un correo, registro de inicios de sesión; toda la información de los perfiles en redes sociales como contactos, seguidores, amigos, fecha y hora de cada publicación, dispositivo utilizado para acceder a la red social, tiempo y hora de acceso; páginas visitadas en internet, etc., en otras palabras, lo que se conoce como huella digital. Estos datos no son considerados

personales, pero eventualmente también permiten individualizar a una persona, por ejemplo, solo hace falta conocer la dirección IP, que es la identificación única de cada dispositivo que se conecta a internet, para saber quién es el titular (González, 2018, p. 276).

Esta distinción entre datos personales y datos de tráfico es relevante en virtud de sus efectos jurídicos. Como se explica en el capítulo cuarto, las normas colombianas relativas a la protección de datos personales solo protegen los datos personales propiamente dichos, ya que son estos los que, en principio, permiten individualizar a una persona y revelar aspectos de su esfera íntima (González, 2018, p. 277).

### *1.4 Multifuncionalidad de la inteligencia artificial y el big data*

Los usos del *big data* y la inteligencia artificial son tan diversos como extensos. Estas herramientas tecnológicas pueden usarse para algo tan simple como determinar la demanda de cada producto de un supermercado y que este optimice la cadena de suministro; o advertir a las empresas los períodos en que se van a producir incrementos y disminuciones en las ventas o notificar al usuario de un banco cuando se ha producido un movimiento sospechoso en su cuenta, e incluso analizar cuándo es más rentable invertir en la bolsa.

El big data es especialmente común en estudios de mercadeo, en los que se identifican los gustos de la persona con base en la información que los usuarios depositan en internet de forma consciente o inconsciente y, posteriormente, se les muestran anuncios o publicaciones que podrían ser de su interés. Por ejemplo, empresas como Amazon realizan segmentaciones de sus clientes y cruzan sus hábitos de compra con los de otras personas con hábitos o gustos parecidos, para sí mostrarles publicidad y boletines de compra o descuentos con aquello que el usuario necesite o esté interesado en comprar (Casas *et al*, 2019, p. 38).

En conclusión “gracias al big data y la inteligencia artificial se permite generar patrones dinámicos de tendencias de futuro: la predictibilidad y el apoyo en la toma de decisiones. Se puede conocer mejor al cliente, al mercado, personalizar los productos y servicios, mejorar y agilizar la toma de decisiones, prever el comportamiento” (Cotino, 2018, p. 133).

Ahora bien, Cathy O´Neill (2017), reconocida matemática e ingeniera de datos, en su libro *Armas de destrucción matemática*, menciona otras aplicaciones un poco más complejas y cuestionables desde el punto de vista ético, las cuales van más allá del ámbito económico y transgreden la esfera interna de quien es objeto de escrutinio por parte de estas herramientas. En ese sentido, estas tecnologías han avanzado hasta poder identificar las probabilidades de que un sujeto en específico incumpla una obligación crediticia con su banco; o en el caso de los modelos de reincidencia carcelarios en Estados Unidos, establecer qué probabilidades tiene el indiciado de un delito de reincidir en su conducta, lo cual permite al juez graduar la pena a imponer; e, inclusive, deducir cuáles son los gustos y preferencias de los electores con la finalidad de establecer qué debe contener un anuncio publicitario para cambiar su forma de pensar frente a un candidato u otro (O'Neill, 2017, pp. 25-35). En el capítulo siguiente, se profundizará en algunos casos que evidencian usos problemáticos de algoritmos de big data e inteligencia artificial.

# 2. CASOS PARADIGMÁTICOS DE USOS PROBLEMÁTICOS DEL BIG DATA Y LA INTELIGENCIA ARTIFICIAL

Ciudadanos, actores privados y Estado convergen en internet, en este nuevo ámbito en el cual los ciudadanos se creían libres, pero el surgimiento de tecnologías como el *big data* han favorecido la interferencia del Estado y de actores privados en el mismo. El internet y las nuevas tecnologías para el procesamiento de datos han producido nuevas formas de interacción entre los ciudadados, nuevas plataformas que estimulan el debate y la confrontación de ideas pero que, en contraposición, también han generado nuevos riesgos para el ejercicio libertades, así como un cambio en las relaciones entre el Estado y el ciudadano.

En este capítulo, se expondrán distintos casos en los que algoritmos de b*ig data* e inteligencia artificial, así como la ingeniería de datos, han sido las herramientas esenciales en la realización de planes de vigilancia masiva, en la creación de publicidad cognitiva dirigida al elector, y en la manipulación a la opinión pública. Estos casos se consideran paradigmáticos debido a que ponen de manifiesto la necesidad de regulación jurídica sobre la forma en la han sido utilizadas estas nuevas tecnologías por actores estatales y no estatales y el reforzamiento de las normas de protección de datos personales.

## *2.1 La red de vigilancia masiva en Estados Unidos*

La primera década del siglo XXI estuvo influenciada por dos fenómenos que se dispersaron a nivel internacional: “por una parte, la disposición de las tecnologías precisas para procesar e interpretar inmensas cantidades de datos y, por otra, una simétrica erosión de la privacidad acentuada por el miedo derivado de los atentados terroristas producidos en los Estados Unidos del año 2001” (González, 2018, p. 281). Los atentados terroristas en Estados Unidos y, posteriormente, los incidentes que tuvieron lugar en Madrid en el 2004 y Londres en el 2005, marcaron la pauta para el uso de datos personales en la lucha contra el terrorismo. En este capítulo, se mencionarán casos en los que el big data y la inteligencia artificial han sido utilizadas por gobiernos para recopilar información sobre los ciudadanos y rastrear la posible comisión de delitos contra la seguridad nacional.

En el caso de los Estados Unidos, de acuerdo con un reportaje de la *BBC* del 2013, el entonces funcionario de la CIA, Edward Snowden, filtró millones de documentos de titularidad de la Agencia Central de Inteligencia (CIA) y la Agencia Nacional de Seguridad (NSA), los cuales dieron a conocer la red de vigilancia masiva de Estados Unidos, cuya finalidad era recopilar, rastrear y monitorear los registros de llamadas telefónicas y datos de tráfico o huella digital de los ciudadanos norteamericanos a través de internet. A partir de los documentos filtrados, se reveló que una corte había impartido una orden judicial que conminaba a Verizon, empresa de telecomunicaciones, a entregar los macrodatos relativos a los registros de llamadas telefónicas a la NSA. Asimismo, se dio a conocer al público que la NSA habría intervenido los servidores de compañías de internet como Google, Facebook, Microsoft, etc. Y, de esta manera, habría rastreado las comunicaciones de los usuarios de estas plataformas. Estos datos eran obtenidos con objetivo de detectar, prevenir y penalizar a aquellos que pudiesen suponer un riesgo para la seguridad nacional (BBC Mundo, 2013).

En ese mismo año, un reportaje de *The Guardian* (2013) reveló que la NSA obtenía acceso directo a los datos que se almacenaban en servidores de internet a partir de un programa llamado PRISM, el cual permitía a los agentes recolectar información como historiales de búsqueda, el contenido de emails y otros chats, archivos transferidos, etc. Con los datos obtenidos, el programa creaba perfiles de los ciudadanos en busca de patrones de criminalidad, clasificando a los individuos según su peligrosidad o potencialidad de cometer un delito. En definitiva, la vigilancia en masa por parte del Estado supone un riesgo para un repertorio de derechos, que será analizado en el capítulo 3.

### *2.2 Los algoritmos en las campañas políticas*

La *Cuarta revolución* ha generado un cambio sustancial en la forma en la que se llevan a cabo las campañas políticas. Más allá de propuestas populistas, el escenario electoral se ha visto permeado por una nueva dinámica donde las estrategias principales consisten en el uso del *big data* y los *fake news*, elementos esenciales para la distorsión de la opinión pública. Estas herramientas “van moldeando tanto las formas de percibir como de interpretar lo

percibido desde las nuevas tecnologías, la psicología social y las ciencias de la comunicación" (Ardini y Nahúm, 2020, p. 229) y constituyen la nueva estrategia para que, quienes cuentan con los medios económicos y políticos, puedan acceder con mayor facilidad al poder.

En este aparte se abordará la manera en que el big data y la inteligencia artificial han sido utilizadas por candidatos políticos en el ámbito electoral, con la finalidad de crear propaganda cognitiva para sugestionar su decisión de voto.

### *2.2.1 Cambridge Analytica y la campaña electoral de Donald Trump*

En el año 2018, el periódico estadounidense *The New York Times*, en colaboración con los periódicos ingleses *The Guardian* y *The observer*, realizó un reportaje sobre las elecciones presidenciales de Estados Unidos de 2016, en el cual se expuso una problemática que cambiaría el paradigma en torno a la protección de datos personales y las herramientas tecnológicas de captación de información. La campaña electoral del entonces candidato a la presidencia Donald J. Trump, contrató a Cambridge Analytica, una empresa inglesa que, a partir del big data y la minería de datos, creaba campañas publicitarias que tuviesen la finalidad de sugestionar el comportamiento de la audiencia a la cual se dirigiesen. Con la finalidad de cambiar la forma de pensar del electorado y lograr el triunfo de Donald Trump en las elecciones, la empresa recolectó datos personales de 57 millones de posibles votantes que fuesen usuarios de Facebook a través de una aplicación que le ofrecía realizar un test de personalidad. Para poder acceder a la aplicación, el usuario debía ingresar su cuenta de Facebook y, al aceptar las cláusulas de los términos y condiciones de uso, otorgaba permiso a Cambridge Analytica para acceder a la información personal de su perfil de Facebook y la de sus amigos (New York Times, 2018; BBC, 2018).

Alexander Nix, consejero delegado de Cambridge Analytica, en una entrevista concedida al diario italiano La Stampa, el 8 de septiembre de 2016, declaró lo siguiente:

> Creo que el modo de hacer campañas electorales está cambiando. [...] Antes se hacía campaña electoral encomendándose a sondeos de opinión y a la intuición de los candidatos y sus

> equipos. Hoy tenemos la posibilidad de utilizar grandes cantidades de datos que nos permiten crear modelos de análisis predictivo de las inclinaciones y del comportamiento. Con esta información podemos identificar y alcanzar con mensajes eficaces a los electores: sabemos cuáles son los temas de interés y por lo tanto hablamos de lo que importa a los votantes, dando matices diferentes a la comunicación para garantizar el éxito de la misma. (*Diario La Stampa*, 2016, como se cita en Betzu *et al*, 2019, p. 261)

El tratamiento de datos personales que se realizó con la finalidad de examinar el comportamiento de la audiencia electoral marcó la pauta en el ámbito de la minería de datos para crear publicidad política personalizada y predecir el comportamiento de la audiencia a la que estuviese dirigida. A continuación, se explicará cuál es el proceso de creación de publicidad cognitiva electoral o personalizada a través de la captación de datos personales en plataformas digitales, prácticas que también representan una amenaza a la privacidad y la autonomía de los ciudadano.

## *I. Recopilación de datos*

Global Science Research (GSR) es una empresa inglesa dedicada a la psicología cuantitativa que fue contratada por Cambridge Analytica para recopilar los datos personales de los usuarios de Facebook en Estados Unidos. Para tal fin, la empresa creó un cuestionario llamado "Thisismydigitalife" a partir de la interfaz de programación de aplicaciones (API) de Facebook. Aproximadamente 270.000 personas ingresaron a la aplicación y tomaron el test, para lo cual en los Términos y Condiciones el aplicativo requería acceder a los datos del perfil de Facebook del usuario y toda su red de amigos, recopilando de esta manera la información de 87 millones de personas[4]. A pesar de la cantidad masiva de datos recopilados, Facebook pasó por alto la captación masiva de datos por parte de GSR, quien alegó que la recolección se hizo con fines académicos. Sin embargo, esta explicación no es satisfactoria porque después transferiría dichos datos a Cambridge Analytica (Metcalf, 2018).

[4] Se recolectaron los datos de 87 millones de personas sobre una población de 214 millones de personas registradas para votar para 2016 y un número de votantes de 140 millones para el mismo año, según la Comisión de Asistencia a las Elecciones (EAC).

## *II. Creación de perfiles psicométricos*

A partir de la cohorte de las 270.000 personas que tomaron el test, Cambridge Analytica creó perfiles psicométricos para conjuntos de personas que compartieran rasgos de la personalidad similares, lo que le permitiría crear anuncios dirigidos votantes de un mismo segmento (Metcalf, 2018). Para tal fin, los datos recopilados a partir del aplicativo del test de personalidad, fueron contrastados con encuestas tradicionales, datos de acceso público –como registros de votantes, número de seguridad social, registro de propiedad-, y datos de tráfico con la finalidad de verificar la veracidad de los datos obtenidos y crear una base de datos más robusta y completa. Entre más datos obtuvieran, más preciso sería el modelo predictivo.

El paso posterior sería crear segmentos o grupos poblacionales cuyo factor diferencial estaba determinado por un cuestionario o test psicométrico[5] conocido como Test OCEAN de los cinco rasgos de la personalidad[6]. En ese sentido, el conjunto de datos de cada individuo sería utilizado para identificar a qué segmento poblacional y sociodemográfico pertenecería la persona. La agrupación según las características psicológicas tendría la finalidad ulterior de desarrollar la propaganda electoral según el perfil de cada sujeto y pronosticar cómo se comportaría el elector ante esta (Metcalf, 2018; González, 2018, p. 283).

Luego de contrastar, verificar los datos y segmentar a los individuos, Cambridge Analytica utilizaría el *big data* y la minería de datos para descubrir correlaciones entre los rasgos de la personalidad y los datos obtenidos de cada posible votante (Por ejemplo, descubrieron correlaciones tan específicas como que los fans del cantante Tom Waits tenían una tendencia a desarrollar una personalidad abierta). El conjunto de datos obtenidos de cada individuo (resultados del test "Thisismydigitalife", datos del perfil de Facebook, datos públicos y datos de tráfico, etc.) permitió crear correlaciones y, adicionalmente, obtener, con una precisión

[5] La psicometría es es un procedimiento de medida objetiva y estandarizada de una muestra de comportamientos (Meneses, 2013, p. 18).

[6] Este modelo fue desarrollado por Michal Kosinski y David Stillwell y se basa en cinco rasgos de la personalidad: apertura a nuevas experiencias, responsabilidad, extroversión, amabilidad e inestabilidad emocional, y parte del supuesto de que cada persona encaja en un espectro bajo o alto para cada uno de estos rasgos (González, 2018, p. 281).

mayor al 95%, datos sensibles como orientación sexual, etnicidad, ideología, tendencia a enfermedades mentales, estados de ánimo, etc. (González, 2018, p. 282).

En conclusión, los perfiles psicométricos no solo se basan en los datos de los electores, sino que permiten inferir más información sobre el sujeto sometido a análisis, y qué tipos de contenidos pueden resultar atractivos para este. Lo cierto es que los algoritmos computacionales tienen la capacidad de establecer correlaciones y hacer predicciones que escapan la capacidad humana. En otras palabras, "permiten identificar en qué profesión un individuo podría tener éxito; o incluso qué estrategia de información podría funcionar mejor para influir sobre el comportamiento de una determinada persona, de manera que compre un cierto producto o vote por algún candidato" (Kosinski, 2017, p.6).

### *III. Micro-targeting o microsegmentación*

Esta técnica de mercadeo consiste en "interactuar y aprender del elector al que tratará de persuadir con argumentos racioemocionales, intentando imitar los intereses personales, sociales y emocionales de este y ofrecer al mismo, variantes de campaña propagandística adaptadas a su perfil psicológico" (González, 2018, p. 284). Este adquiere su nombre porque tiene por objetivo agrupar a los electores en pequeños segmentos de personas que comparten el mismo perfil psicométrico, aprender de este y entender cómo responde cada grupo a la publicidad (González, 2018, p. 285). El *big data* y la inteligencia artificial fueron utilizados conjuntamente en este escenario para aprender en tiempo real cómo el elector responde a la publicidad, para así readaptarse y perfeccionar el modelo.

Con la finalidad de potenciar el modelo, Cambridge Analytica creó cincuenta mil variantes de distintos lemas y argumentos electorales, los cuáles eran repartidos en un radio de 5 millas de acuerdo con el perfil psicométrico. Diariamente, eran puestos a prueba alrededor de 175.000 anuncios. A su vez, a través de herramientas de Facebook que permiten predeterminar públicos personalizados y similares para orientar la publicidad, el *micro-targeting* permitió a los dirigentes de la campaña identificar qué anuncios personalizados se convertirían en tendencias entre las personas de un mismo segmento (Metcalf, 2018).

Luis González (2018) destaca que las variantes de la campaña electoral no pueden ser conocidos por otros electores pertenecientes a un segmento distinto, ni mucho menos por autoridades electorales, debido a que estas son repartidas a sus destinatarios a través de publicaciones invisibles, es decir, son anuncios en páginas web que solo pueden ser conocidos por el perfil que la recibe y no pueden ser compartidos (p. 280).

## *IV. Fake news*

Siguiendo la línea argumentativa del autor Luis González (2018), a la propaganda cognitiva electoral se le suma otro fenómeno de distorsión de la opinión pública y es la dispersión de fake news y la manipulación de *trendig topics* a través de *bots*, que hacen referencia a la creación artificial de tendencias en redes sociales a partir de sistemas automatizados a la merced de sus creadores. Esta táctica fue igualmente utilizada en la campaña de Donald Trump en conjunto con la microsegmentación, a fin de desinformar a segmentos específicos de la población, difundiendo información falsa sobre contrincantes políticos. A partir de esta estrategia, surgió la campaña de desprestigio conocida como *Crooked Hillary* contra la candidata Hillary Clinton. De acuerdo con CNN news, Alexander Nix, CEO de Cambridge Analytica, aceptó haber orquestado el crecimiento viral de dicha iniciativa a través de la red social Twitter, compartiendo noticias falsas sobre la ex candidata a la presidencia, tales como el supuesto financiamiento de su campaña por parte del gobierno ruso, o sobre su supuesto apoyo a la guerra de Iraq.

Como se ha mencionado hasta el momento, la aplicación de estas herramienta tecnológica es útil en la medida en que permite tomar decisiones más efectivas basadas en los datos. Pero, aparte del juicio de utilidad y conveniencia, es importante cuestionar en qué medida es deseable y legítimo que las empresas, el gobierno y los candidatos a elecciones empleen este tipo de algoritmos para predecir aquello que lo que los ciudadanos son proclives a hacer y pensar; y cómo el uso de datos personales para la creación de publicidad política personalizada puede afectar los ideales de un Estado democrático, bajo la premisa de que se trata de herramientas capaces de predecir el comportamiento de los ciudadanos y, de acuerdo

con su perfil psicológico, utilizar los argumentos adecuados para persuadirlos de realizar cierta acción, como en este caso, votar, afectando de esta forma su libertad individual.

### *2.2.2 Los algoritmos en el contexto electoral latinoamericano*

La región latinoamericana no está exenta de los avances tecnológicos. De hecho, este escenario de poca cohesión social y política es el contexto que propició nuevas dinámicas de distorsión de la opinión pública: los *fake news* y el *big data*. En ese sentido, se hará un recuento de los casos en los que se ha utilizado el *big data* en el escenario electoral y en el contexto de la protesta social a lo largo de la región con la finalidad de difundir noticias falsas y de esta forma intervenir en la opinión y el debate público.

#### *I. El caso argentino*

En junio de 2018, de acuerdo con un informe presentado por la Comisión de Asuntos Digitales, Cultura, Medios y Deporte del Parlamento británico (https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36309.htm), Alexander Nix, el CEO de Cambridge Analytica, admitió haber diseñado una campaña de desprestigio contra la ex presidenta Cristina Fernández de Kirchner. La investigación llevada a cabo por el Parlamento Británico concluyó que la empresa habría contratado oficiales retirados de agencias de inteligencia de Israel, EE. UU., Reino Unido, España y Rusia con la finalidad de adelantar labores de inteligencia; asimismo, habrían creado cuentas falsas de Facebook y twitter para apoyar la campaña contra Kirchner.

El papel de Cambridge Analytica en dichas elecciones consistió en polarizar al electorado, principalmente sembrando odio hacia el candidato opositor. El *modus operandi* en Argentina en el 2015 no fue distinto del utilizado en las elecciones estadounidense del 2016; de acuerdo con un reportaje del diario argentino *La Nación* (2019), la función que desempeñó la empresa de minería de datos consistió en determinar qué votantes eran fervientes opositores del Partido Propuesta Republicana y, por tanto, no valía la pena gastar recursos en ellos, y cuáles podrían considerarse como votantes indecisos, los cuáles serían el público objeto de la publicidad política personalizada. De acuerdo con el diario argentino, Cambridge Analytica

no fue el responsable de la creación de la publicidad personalizada, toda vez que fue el partido Propuesta Republicana quien realizó esta tarea con medios propios.

## *II. El caso brasilero*

Fueron varios los factores que determinaron el ascenso a la presidencia de Jair Messias Bolsonaro en el año 2018, a saber: el *impeachment* de Dilma Rousseff, el encarcelamiento de Ignacio Lula Da Silva y el uso del *big data* a través de la red social de mensajería WhatsApp. Las empresas proveedoras de datos en Brasil, fueron las principales colaboradoras de la campaña a la presidencia de Bolsonaro. El acceso al *big data* permitió que los mensajes propagandísticos se propagaran a través de grupos y cadenas de WhatsApp, difundiendo *fake news* sobre los opositores políticos pertenecientes al *Partido de los trabajadores* (Ardini y Nahúm, 2019, p.231).

En ese sentido, la estrategia de utilizar la plataforma de mensajería de WhatsApp jugó a favor del candidato en cuestión por dos razones: en primer lugar, el servicio de mensajería no está sometido a control alguno en materia de propaganda política debido a que el contenido de los mensajes es completamente libre, lo que le otorgó a la campaña la posibilidad de difundir cualquier tipo de mensaje difamatorio y, en segundo lugar, este es el medio mediante el cual la mayoría de sectores populares se informa sobre asuntos políticos (Ardini y Nahúm, 2019, p. 231)

## *III. Las protestas en Chile y Colombia*

"Con las particularidades de cada caso, la protesta popular también intentó ser desarticulada y descalificada por parte de sus respectivos gobiernos y a partir del uso de una represión atroz por parte de las fuerzas policiales, pero también con la proliferación incesante de *fake news* a través de las redes sociales virtuales" (Ardini y Nahúm, 2019, p. 232).

De acuerdo con el reportaje *La mano negra tras la crisis de Chile y Colombia* del periódico español El Mundo, Alto Analytics, empresa consultoria de análisis de datos, realizó un examen sobre 101 millones de mensajes provenientes de 7,6 millones de cuentas de Twitter,

el cual indicó que solo un pequeño porcentaje de esas cuentas (el 1% en Colombia y el 0,5% en Chile) generó alrededor del 30% de los contenidos que circularon durante las protestas en ambos países (33% en Colombia y 28% en Chile). El informe también indica que medios internacionales que participan en campañas de propaganda como Russia Today o TeleSur, así como Cuba Debate y EVTV Digital también intervinieron con narrativas polarizantes.

En ese sentido, el estudio elaborado encontró que 1% de cuentas que creó el 33% de los contenidos en Colobia, eran simples cuentas de Facebook o Twitter con la apariencia de medios de comunicación pero sin ningún tipo de estructura empresarial. En el caso de la red social Facebook, esta red social fue utilizada para difundir 135 convocatorias en Chile y 53 convocatorias en Colombia para manifestarse en contra del gobierno. Asimismo, en el análisis se realizó una depuración estadística que permitió identificar 175 cuentas que intervinieron tanto en las protestas de Colombia como en las de Chile, de las cuales se pudo geolocalizar 125 de ellas y se encontró que el 58% estaban situadas en Venezuela.

Las conclusiones de Alto Analytics son consistentes con el informe realizado por el Departamento de Estado de Estados Unidos, el cual encontró que cuentas de Twitter y otras redes sociales provenientes de Venezuela y Rusia fueron utilizadas para incidir en el debate público y generar inestabilidad. Las anomalías expuestas surgen a tarvés de variadas redes sociales, desde WhatsApp, Twitter, Facebook, Youtube, lo cual pone de presente los riesgos que el uso de redes sociales implica para la formulación de la opinión pública (El mundo, 2020).

Los problemas en torno a la difusión de fake news como estrategia para incidir en la opinión pública se exacerban con los procesos de personalización masiva de la información que hoy se permiten con las redes sociales y el big data. El principal motor de la difusión de contenidos es la homofilia: la tendencia a compartir información de usuarios que presentan un perfil similar al propio. Lo anterior conduce necesariamente a severos errores en la formación de la opinión pública en segmentos poblacionales, lo que favorece extraordinariamente la difusión de fake news en masas de público polarizado y la creación de sesgos de confirmación (Cotino, 2018, p. 290-296).

# 3. PROBLEMÁTICAS DEL USO DE ALGORITMOS TECNOLÓGICOS PARA LOS DERECHOS HUMANOS, LA AUTONOMÍA Y LA DEMOCRACIA: UN ANÁLISIS CONCEPTUAL

En este capítulo se realizará un análisis teórico y conceptual, más que jurídico, sobre los posibles riesgos que el uso de algoritmos implica para los derechos humanos y otros valores como la autonomía y la democracia. Este capítulo se dividirá en dos partes: la primera, hará referencia a los problemas que suscita el uso del *big data* y la inteligencia artificial para la privacidad y la protección de datos personales. En segundo lugar, se analizarán los problemas que derivan de la naturaleza y diseño de la tecnología, esto es, la opacidad y los sesgos implícitos, los cuales, si bien están relacionados con el uso de datos personales, se presentan con independencia de que los últimos hayan sido recolectados legítimamente y su tratamiento haya sido autorizado, derivando en posibles consecuencias para la igualdad, la autonomía y la democracia.

## *3.1. Los potenciales riesgos para la privacidad y los datos personales*

El avance de las tecnologías de procesamiento de la información supone grandes retos para la privacidad en razón de la escala y metodologías de análisis. En ese sentido, el análisis los casos expuestos en el capítulo anterior permite identificar un patrón en la manera en que se realiza el procesamiento de datos. En todos los casos fue necesaria, en primer lugar, la i) recolección datos de tráfico o datos personales de los usuarios de internet sin conocimiento o consentimiento del titular y ii) la deducción de otros datos personales o de comportamientos del individuo.

La recolección de datos sin el conocimiento o consentimiento del titular y la predicción de otros datos personales o de comportamientos del individuo, son considerados como los mayores retos para la privacidad y la protección de datos personales que se asocian al uso de algoritmos, específicamente, en relación con el consentimiento informado y la forma en que se obtienen datos sensibles. En este capítulo se analizarán qué aspectos de la recolección y inferencia de datos suponen riesgos para la privacidad.

El concepto de privacidad como derecho tiene su origen en el ensayo *The right to privacy* de Samuel Warren y Louis Brandeis de 1890 que define el derecho la privacidad como la protección de lo que en español llamaríamos la intimidad de las personas, es decir, pensamientos y sentimientos en cualquier forma o expresión, y que consiste en la potestad de decidir si se le da o no publicidad y hasta qué punto (Toscano, 2016, p. 540).

> En 1948, el derecho a la intimidad fue reconocido por primera vez en el derecho internacional en la Declaración Universal de los Derechos Humanos, cuyo artículo 12 dispone que toda persona debe ser protegida contra injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación. Posteriormente, en 1966, este precepto fue reproducido por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). A nivel regional, en el sistema interamericano, el derecho fue consagrado en el artículo 11 de la Convención Americana de Derechos Humanos de 1969, el cual reproduce el art. 12 de la Declaración Universal. En cuanto al sistema europeo, el derecho a la intimidad fue reconocido por primera vez en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en 1950 (Sentencia C-748 de 2011).

Asimismo, se parte del supuesto de que los retos para la privacidad también son retos para la protección de datos personales en tanto el derecho a la privacidad o intimidad está estrechamente ligado al derecho de habeas data. Riascos Gómes (1999, p. 34) explica la relación entre ambos derechos desde una perspectiva filosófica según la cual "el derecho a la privacidad es un derecho de la persona que fomenta y desarrolla la personalidad con atributos y poderes para oponerse a lo público, para exigir la no intromisión, indiscreción ajena vistas, escuchas y captaciones de datos personales por cualquier medio tecnológico de la información y la comunicación o TIC y/o informático" (p. 34).

Las normas jurídicas europeas en materia de protección de datos personales son el esquema de protección de mayor desarrollo y trayectoria. La protección de datos personales surge a partir del Convenio 108 del Consejo de Europa, el cual brinda protección explícita a los datos

personales y fija las pautas para establecer un modelo europeo de protección de datos. Este instrumento concibe el derecho a la protección de datos como un mecanismo de defensa de la esfera privada del individuo ante el auge de las tecnologías de la información. Posteriormente, en 1995, el Parlamento Europeo y el Consejo de Europa, expidieron la Directiva 95/46/CE sobre la protección de personas físicas respecto al tratamiento y circulación de datos personales con el objeto de dotar de contenido los principios del derecho a la privacidad ya contemplados en el Convenio 108[7], así como para ampliarlos y armonizar la legislación referente a la protección de datos en los Estados miembros de la Unión europea (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2014, p. 19).

Posteriormente, derecho de habeas data fue consagrado como un derecho autónomo con en la Carta de los Derechos Fundamentales de la Unión Europea de 1999, cuyo art. 8 lo concibe de la siguiente manera:

> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.
>
> 3. El respeto de estas normas estará sujeto al control de una autoridad independiente.

En otras palabras, el derecho de habeas data confiere una potestad a su titular que le permite determinar el uso y destino de sus datos personales con la finalidad de evitar su tráfico ilícito y lesionar su dignidad. Asimismo, la protección de este derecho impone deberes en cabeza de quienes realicen el tratamiento de los datos personales, tales como la obtención del previo consentimiento para su recolección y uso, informar sobre el destino y la finalidad de recolección de esos datos y la posibilidad de que rectificarlos o cancelarlos (Cotino, 2018, p. 144).

---

[7] El art. 11 del Convenio 108 contempló la posibilidad de incluir otros instrumentos de protección. Dicha norma fue el fundamento de la Directiva 95/46/CE expedida por el Parlamento Europeo y el Consejo Europeo.

El reconocimiento del derecho al habeas data, como un derecho autónomo, persigue la protección de los datos personales en un mundo globalizado en el que el poder informático es creciente. Se otorga esta protección debido a la relevancia que estos datos suponen para la garantía de otros derechos como la intimidad, el buen nombre y el libre desarrollo de la personalidad, razón por la que los retos para la protección de datos personales también son retos para la intimidad o privacidad (Sentencia C-748 de 2011).

Ahora bien, las normas comunitarias europeas son el marco normativo de mayor desarrollo en protección de datos personales. La Unión Europea ha trabajado en adaptar sus regulaciones a la era digital, actualizando sus normas de conformidad a los nuevos retos que plantean las tecnologías emergentes para los datos personales. El Reglamento General de la Unión Europea de Protección de Datos Personales (RGDP), expedido el 25 de mayo de 2018, en su considerando 7, plantea que los avances tecnológicos 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. Por esta razón, las categorías jurídicas que sean objeto de análisis en este trabajo, tales como la definición de datos personales y la garantía de consentimiento informado, se definirán en relación con las normas comunitarias europeas debido a que estas constituyen el paradigma de protección de datos personales (Agencia de los Derechos Fundamentales de la Unión Europea y Consejo de Europa, 2014, p. 19). Es decir, el RGDP será el referente conceptual en este capítulo.

Es de suma importancia resaltar que el aparte 3.1 tiene como finalidad analizar qué aspectos del la recolección y predicción de datos a partir del *big data* suponen un riesgo potencial para la privacidad, usando como punto de partida los estándares de protección de datos personales de las normas comunitarias europeas debido a que son las más estrictas y las de mayor desarrollo en materia de protección de datos personales hasta el punto de ser el marco jurídico paradigmático en dicha materia (González Guerrero, 2018, p. 215), más no tiene como finalidad argumentar la vulneración de un precepto normativo específico.

### *3.1.1 La recolección de datos personales sin conocimiento o consentimiento del titular*

Al hacer uso del internet, el control por parte del individuo sobre sus datos puede perderse fácilmente ya que en muchos casos ni siquiera es consciente del procesamiento o no puede rastrear cómo sus datos son transferidos de un servidor[8] a otro. Cuando el usuario acepta los términos y condiciones o las políticas de privacidad de una página web, los datos – personales o de tráfico- son almacenados en un servidor y se vuelve una tarea casi imposible rastrear sus usos y tratamientos, debido a que la información puede ser almacenada en forma de cookies[9], puede ser objeto de intercambios comerciales, o de rastreo de por parte de terceros[10]. El *big data* es la herramienta que permite almacenar los datos captados por los distintos servidores y crear perfiles de conducta, de consumo y de hábitos personales (González Guerrero, 2018, p. 213), lo cual plantea importantes desafíos sobre cómo informar de manera efectiva y oportuna a los usuarios sobre el procesamiento de datos personales y sobre quién está a cargo de esta tarea (ENISA, 2015, p. 13).

Es errado considerar que cada persona, al aceptar los términos y condiciones que se requieren para el uso de cualquier aplicación, sitio web o red social, accede consciente y libremente a que se recopilen sus datos y se sometan a análisis por las siguientes razones: en primer lugar, los términos y condiciones de acceso a plataformas electrónicas son innegociables, son un típico contrato de adhesión en el que la voluntad de quien lo suscribe se limita a establecer si los acepta o no. En segundo lugar, el acceso a internet es una tan necesario que sería irreal pensar que la sociedad está dispuesta a renunciar a la tecnología con la finalidad de proteger su privacidad y la seguridad de sus datos.

---

[8] Un servidor es un ordenador u otro tipo de equipo informático que se ocupa de suministrar información a una serie de clientes, ya sean personas u otros dispositivos conectados a él. Los datos que puede transmitir son variados y múltiples, desde programas informáticos, bases de datos, archivos de texto, imagen o vídeo, etc (García, 2018).

[9] Las cookies son archivos de texto que guardan información sobre las acciones del usuario; los servidores leen esta información para recordar lo que se hizo en cada clic anterior (González Guerrero, 2018, p. 213).

[10] Al visitar portales en la web, se instalan dos tipos de *cookies*. Las primeras son de los servidores de las páginas que el usuario visita directamente. Las segundas son las que instalan servidores ajenos, llamadas *cookies* de terceros y que permiten el rastreo de los hábitos de navegación de las personas (González Guerrero, 2018, p. 214).

Adicionalmente, uno de los objetivos principales de la analítica del *big data* es combinar datos personales, datos de tráfico, bases de datos de distintas fuentes y almacenar nuevos datos de manera continua, de tal forma que el resultado de los análisis sea cada vez más preciso. Por lo tanto, el procesamiento de datos personales no representa el único reto para la privacidad en tanto los metadatos, que son datos de acceso público y, por lo tanto, no gozan de la misma protección legal que los datos personales, también permiten individualizar a una persona y permitir realizar catalogaciones, perfiles, agrupaciones, etc. (ENISA, 2018, p. 13).

Por último, sería una falacia argumentar que todo tratamiento de los datos que pueden atribuirse a una persona, fue consentido por esta. En la Unión europea, las normas en materia de protección de datos personales exigen que cuando se realice el tratamiento de los datos personales se obtenga un consentimiento libre e informado11 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 (Martínez, 2019, p. 17). El uso del big data hace que la garantía del consentimiento que exige que se especifique de la forma más detallada posible qué datos serán recopilados y para qué finalidad, sea inmaterializable porque es poco factible que una persona consienta el tratamiento de una cantidad incalculable de datos.

El Tribunal constitucional colombiano en la Sentencia No. T-176 de 1995, indica como tesis que para que exista una vulneración del derecho al habeas data, la información recolectada debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato, ser errónea o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (Cervantes Días, 2009, p. 33). El problema para la privacidad y el derecho de habeas data radica en que el internet permite la transferencia de datos sin control alguno por parte del titular y el *big data* y la inteligencia artificial facilitan el análisis y

[11] El consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen (Art. 4, RGDP).

procesamiento de esos datos sin consentimiento del mismo. Si bien cada individuo está constantemente realizando concesiones sobre su información en la red, debido a la falta de control y garantías sobre el uso que se les da a los datos, esto no podría entenderse como el ejercicio de la facultad que otorga el derecho a la privacidad de decidir libremente qué información se decide exteriorizar y cuál no.

### *1.1.2 Deducción de datos personales sensibles y otros comportamientos*

Hoy en día la industria de datos conoce cada vez más las inclinaciones psicológicas y los aspectos más íntimos de las personas. El problema para el derecho a la intimidad y el derecho de habeas data radica en que esta información no se obtiene directamente del titular, sino que se predice a partir de los comportamientos en línea (González, 2018, p. 223). El *big data* y la inteligencia artificial permiten deducir datos personales sensibles a partir de análisis predictivos y la contrastación con datos de distintas fuentes. El problema radica en que esta deducción de datos permite revelar aspectos íntimos de la vida de una persona sin que esta sea la que los revele.

Michal Kosinski (2017), psicólogo de comportamiento organizacional de la Universidad de Stanford, quien ideó el Test OCEAN de los cinco rasgos de la personalidad que se utiliza para la creación de perfiles psicométricos, realizó un estudio para comprobar la efectividad de los algoritmos computacionales para deducir la personalidad de un individuo. Para tal fin, contrastó los resultados de una encuesta tradicional, tomada por el individuo en cuestión, familiares, colegas y amigos, con una estimación de la personalidad de este a partir de *likes* de Facebook. Las conclusiones fueron las siguientes:

> Para estimar el carácter de un individuo, el algoritmo computacional necesita solo 10 *likes* de Facebook para ser más preciso que los compañeros de trabajo. En tanto 100 *likes* le permiten ser más exacto que un familiar o un amigo. Con 250 *likes* el algoritmo es más certero que un cónyuge (Kosinski, 2017, p.7).

Según Michal Kosinski (2017, p. 7) los análisis predictivos son posibles gracias a que cada actividad sencilla que se realiza en una red social, cada palabra que se introduce para actualizar el estatus de Facebook, cada compra realizada en internet constituye un pedazo de

información que permite revelar la personalidad (…). Entre más *likes* se puedan obtener del perfil de un usuario, más exacta se vuelve cualquier predicción. Este estudio evidencia la factibilidad de los algoritmos y, por consiguiente, de sus propietarios para conocer la esfera íntima del individuo sin necesidad de optar por métodos coercitivos para obtener confesiones orales, o sin la necesidad de recolectar la información directamente del titular, sino a través de refinados análisis de sus datos de tráfico y del rastreo automático y sistemático de su conducta en la red (González, 2018, p. 272).

En un estudio realizado por Telenor Group Research, MIT Media Lab, Flowminder Foundation y Stockholm School of Economics sobre la posibilidad de estimar si una persona estaba empleada o no de acuerdo con sus metadatos, se llegó a la siguiente conclusión:

> Una de las nuevas fuentes de datos más prometedoras para hacer predicciones son los registros de redes de telefonía móvil, que tienen el potencial de entregar información casi en tiempo real del comportamiento humano a escala individual y social. Las predicciones de los metadatos de los teléfonos móviles son enormes dado que más de la mitad de la población mundial ahora posee un teléfono móvil. (…) Los datos de la telefonía móvil han demostrado proporcionar indicadores indirectos para evaluar los niveles regionales de pobreza, analfabetismo, estimaciones de población, migración humana, y propagación de epidemias. A nivel individual, los datos de teléfonos móviles se han utilizado para predecir, entre otros, el estado socioeconómico, la demografía y la personalidad (Montjoye et al, 2013, p. 1).

La capacidad de los algoritmos de realizar predicciones es tan compleja que hoy en día es posible identificar aspectos de la personalidad a partir del reconocimiento facial. Aunque en el ámbito académico hay escepticismo sobre la capacidad de extraer aspectos íntimos del individuo con base en el rostro, lo cierto es que este constituye un buen indicador para determinar factores genéticos, hormonales, de desarrollo, del entorno y culturales. Los algoritmos actuales han evolucionado hasta el punto de detectar estas diferencias, que son imperceptibles ante el ojo humano. Kosinski (2017) indica que “lo anterior, permite que a partir de la información de múltiples rostros se entrene a una computadora con algoritmos de

inteligencia artificial para estimar los rasgos individuales con gran precisión, esto permite que el grado de exactitud de una computadora para estimar la personalidad a partir del rostro, sea comparable con el resultado de un cuestionario de personalidad" (p. 7).

En el año 2012, el periódico *The New York Times* publicó un artículo en el que reveló que la cadena de supermercados *Target* había utilizado técnicas de minería de datos para predecir qué clientas estaban embarazadas, incluso si aún no lo habían anunciado públicamente. Esta actividad resultó en la divulgación no autorizada de datos personales debido a que la empresa utilizaba la minería de datos para establecer cuándo una posible clienta estaba embarazada y posteriormente su nombre era revelado a los departamentos de marketing correspondientes para enviar cupones y códigos de descuento a las posibles clientas en estado de embarazo, prediciendo los datos personales sobre ellas en lugar de recopilarla directamente (Crawford y Schultz, 2014, p. 95).

Lo anterior es solo un ejemplo más de la capacidad de los algoritmos de hacer predicciones y deducciones de datos personales sensibles es de suma importancia mencionar porque, cuando se habla de vulneraciones a la privacidad, se piensa únicamente en el resultado de las elecciones o en campañas de marketing, sin tener en cuenta que estas mismas tecnologías están al alcance de los Estados en contextos donde las personas no gozan de la misma libertad y donde la privacidad jugaría un papel con consecuencias mortales. Por ejemplo, con base en imágenes del rostro, un algoritmo podría distinguir entre personas heterosexuales y homosexuales con una precisión del 92%, lo que supone un gran riesgo para aquellos que viven en países donde la homosexualidad es un delito y se castiga con pena de muerte (Kosinski, 2017, p. 10).

Hasta ahora, de la recolección de datos y de la predicción de datos y otros comportamientos podemos concluir que el titular el titular de los datos personales no cuenta con el control efectivo sobre sus datos debido a que internet facilita la transferencia de datos sin control alguno por parte del titular y el *big data* facilita el análisis y procesamiento de esos datos sin consentimiento del mismo.

En segundo lugar, datos como como números de teléfono, localizaciones, direcciones IP, direcciones de email, duraciones de las llamadas o comunicaciones, etc. no suelen ser considerados datos personales pues no están vinculados con una persona sino con las direcciones IP y los identificadores similares del dispositivo utilizado, lo cual es problemático debido a que también permiten realizar análisis y predicciones a nivel colectivo o a nivel personal a partir del *machine learning* y, dependiendo de si la legislación en concreto les otorga la categoría de dato personal, no estaría protegido por las normas de datos personales (Ángel y Newman, 2019, p. 30)

Datos como la hora en la que se envía un correo, la lista de amigos en Facebook, la hora en que se toma una fotografía, no permite identificar a nadie, pero el conjunto de estos, combinado con "el conocimiento contextual y de fondo, así como la correlación cruzada con las bases de datos disponibles públicamente, permite volver a identificar los registros de datos individuales" (Narayanan & Shmatikov, 2007, p. 1 como se cita en González Guerrero, 2019, p. 219). En conclusión, estos datos, con ayuda de algoritmos de análisis predictivo, permiten individualizar e identificar al titular de estos datos, pero sin las garantías de protección de datos personales. Por lo tanto, es importante que estos sean reconocidos expresamente como datos personales debido a la posibilidad de revelar y deducir datos personales a partir de estos.

Ahora bien, en relación con la garantía del consentimiento informado definida en el art. 6 del RGDP condiciona la licitud del tratamiento de datos personales a qur el interesado de su consentimiento para uno o varios fines específicos**.** De conformidad con esta normatividad, es necesario asegurar el mayor grado de detalle posible al respecto de las finalidades de procesamiento de la información. Es necesario reforzar estos preceptos ante la naturaleza y desarrollo del *big data* e inteligencia artificial, que hace difícil determinar de antemano las finalidades o comunicaciones que van a producirse. Los sistemas de inteligencia artificial y decisiones automatizadas hacen que sea difícil consentir respecto de unas finalidades de uso de los datos que por lo general ni se conocen, ni se sospechan (Cotino, 2014, p. 144). Es decir, el *big data* tiene el potencial de eludir la garantía del consentimiento. Desde el momento en el que los datos son recogidos, no siempre es posible saber cuál será el resultado del análisis. Recordemos que los algoritmos pueden desarrollar reglas para clasificar nueva

información en categorías preexistentes o no usar ninguna regla con la finalidad de encontrar patrones o correlaciones (Casas *et al*, 2018, p. 71; Holmes, 2017, p. 20). En este segundo caso, el consentimiento sobre el procesamiento de los datos personales tendría una finalidad indeterminada debido a que los resultados de los análisis son por lo general desconocidos, tanto para el titular de los datos como para el encargado de su tratamiento de los datos.

### *3.2 Los problemas que derivan del diseño de los algoritmos: la opacidad y los sesgos implícitos en perfiles y decisiones automáticas.*

Tanto la creación de bases de datos como los algoritmos reflejan juicios de valor, entre otros, sobre datos, conexiones, inferencias, interpretación y umbrales de inclusión que promueven un propósito específico. Así como los mapas que representan el entorno físico de diversas maneras para satisfacer diferentes necesidades (montañismo, turismo o compras), los algoritmos que crean clasificaciones que no son neutrales ni objetivas debido a que están sesgados hacia sus propósitos y no dan explicaciones de sus decisiones. Es decir, se dice que los algoritmos contienen sesgos porque reflejan los valores implícitos y explícitos de sus diseñadores y permiten la clasificación de los ciudadanos en ideologías, niveles de renta, tipos de conducta expresadas por un seguimiento preciso o constante de sus intereses y estos perfiles son el fundamento de la toma de decisiones automatizadas (Dwork y Mulligan, 2013, p. 34).

En ese sentido, el consentimiento no tiene relación alguna con la producción de desigualdades, la creación de ciclos de retroalimentación injustos o la privación de derechos con fundamento en decisiones automatizadas en razón de la opacidad de los algoritmos (Dwork y Mulligan, 2013, p. 34). Es decir, la protección de datos personales es, en estos supuestos, insuficiente para afrontar los problemas que surgen a partir de la opacidad y falta de neutralidad de los algoritmos que da lugar a la creación de perfiles y la subsiguiente toma de decisiones.

Las circunstancias mencionadas, esto es, los sesgos implícitos, se ven agravadas por la opacidad de los algoritmos. Esta característica se opone a la transparencia y hace referencia a la imposibilidad de conocer el tratamiento que recibe la información, los datos que utiliza

y el valor de cada variable que fundamenta las decisiones, debido a que ni siquiera sus diseñadores pueden prever la manera en la que un algoritmo toma sus decisiones, lo que se conoce como el efecto de la caja negra (*black box effect)*, y, adicionalmente, están protegidos bajo el manto de una patente, del derecho de autor o secreto industrial (Comisión Europea, 2020, p. 12; O'Neill, 2017, p. 73).

El efecto de la caja negra hace referencia a que es imposible establecer cómo un algoritmo que ha interiorizado cantidades masivas de datos toma decisiones en razón de su complejidad. Es decir, en la mayoría de ocasiones no hay manera de trazar el proceso mediante el cual un algoritmo entrenado con inteligencia artificial llega a sus decisiones o predicciones. Se puede establecer cuál es el objetivo general del algoritmo, por ejemplo, maximizar ganancias de un modelo de negocio, pero la forma en que llega a ese objetivo no es clara ex ante ni siquiera para sus creadores (Bathaee, 2018, p. 890-892).

La opacidad y los sesgos implícitos son especialmente visibles en la creación de perfiles y en la posterior toma de decisiones automatizadas con fundamento en estos últimos. La creación de perfiles se describe como el proceso de descubrir conocimiento en bases de datos. Este procedimiento requiere: la recolección de datos; la el rastreo de datos y la combinación de distintos tipos de datos; la identificación de patrones en los datos; interpretación de resultados; y creación del perfil. La creación de perfiles automatizada es nueva de tres maneras. Primero, estos perfiles son creados a partir del *big data* o la inteligencia artificial. Básicamente, estos algoritmos permiten recuperar correlaciones inesperadas en bases de datos que recogen datos de diferentes tipos. En segundo lugar, la creación de perfiles no hace referencia a realizar consultas en bases de datos, resumiendo los atributos de categorías predefinidas, sino de descubrir conocimientos, correlaciones o predicciones con las que no se contaban. En tercer lugar, debido a las características de los algoritmos como la opacidad, no es posible conocer anticipadamente la manera en que la creación de perfiles impacta las acciones de los individuos porque no hay acceso a la forma en que las decisiones se producen y utilizan. Esta última diferencia sugiere que la elaboración de perfiles obstaculiza nuestra libertad para actuar de manera autónoma, sobre este punto se profundizará más adelante (Hildebrandt, 2008, p. 4-5).

La opacidad y los sesgos en los algoritmos pueden fundamentar diferentes tipos de decisiones que, para efectos de su análisis en este capítulo, se dividen en decisiones discriminatorias, decisiones que son desconocidas por el individuo, o decisiones con efectos jurídicos para el individuo. En estos casos, las personas afectadas por estas decisiones pueden carecer de los medios para verificar cuál es el fundamento de una decisión tomada o en la cual intervino un algoritmo. Asimismo, pueden enfrentar dificultades con el acceso efectivo a la justicia en situaciones en que tales decisiones pueden afectarlas negativamente debido a la dificultad de probar si en el caso concreto se vulneró algún derecho o alguna norma (Comisión Europea, 2020, p. 12). Por último, es claro que las problemáticas que se expondrán a continuación también están relacionadas con la protección de datos personales, pero los efectos y posibles afectaciones a otros derechos se producen con independencia de la legalidad con la que se recolecten los datos.

### *1.2.1 Decisiones discriminatorias*

Las decisiones automáticas, tales como la diferenciación de precios o la exclusión de productos y servicios, pueden ser discriminatorias hacia ciertos grupos poblacionales. Aunque los algoritmos detectan patrones en conjuntos grandes de datos, muchas bases de datos históricas contienen sesgos debido a años de prácticas de recolección problemáticas (INCLO, 2018, p. 8). Por ejemplo, los departamentos de policía en Estados Unidos utilizan datos históricos para determinar en qué lugares y a qué hora es más probable que se cometa un delito, con la finalidad de economizar costos en la labor de patrullaje. Las predicciones que hagan estos algoritmos sobre las áreas geográficas con mayor probabilidad de que se cometan delitos, harán que se produzcan más arrestos en estas zonas. Si lo que busca el algoritmo es predecir delitos relativos a la mendicidad, microtráfico, consumo de sustancias, es claro que estos delitos son endémicos de las áreas más empobrecidas de una ciudad, por lo cual se generarán más arrestos. El creador de dicho software, insistió en que el modelo era ciego a la raza y etnia, pues no se centra en personas, sino en un análisis de la geografía, los datos que se usan son la tipología y localización de cada delito. Por desgracia, un mapa de delincuencia generado en este modelo es en realidad un mapa que traza la pobreza y refuerza

la creencia de que son las personas pobres las que cometen la mayoría de delitos en una ciudad (O'Neill, 2017, p. 56).

Por otro lado, en Estados Unidos, las leyes federales prohíben la discriminación en el acceso al crédito. Aún así, la industria de préstamo de créditos ha utilizado el *big data* para identificar y evadir usuarios de internet con bajas calificaciones crediticias al publicar publicidad. Esta misma práctica es utilizada en la industria de bienes raíces, que prohíbe discriminar inquilinos y compradores en razón de su raza, sexo, religión, etc. La policía monitorea los avisos publicitarios en busca de lenguaje específico que sea indicativo de prácticas discriminatorios, pero el *big data* permite a la industria de préstamos de créditos focalizar la publicidad evitando a posibles inquilinos en razón de su raza, sexo, religión, etc. (Crawford y Schultz, 2014, p. 101).

La sociedad está llena de desigualdades y el *big data*, al ser un modelo programado por humanos, es una representación de esa realidad que conlleva a que estas creencias se perpetúen bajo la falsa premisa de que los modelos, al ser automáticos, son transparentes. Es importante traer mencionar que este tipo de prácticas contrarían el principio de igualdad, el cual, en términos generales, ordena dar un trato igual a quienes se encuentran en la misma situación fáctica, y un trato diverso a quienes se hallan en distintas condiciones de hecho (Sentencia C-178 de 2014). En ese sentido, la distinción de trato jamás puede tener un fundamento discriminatorio, toda vez que el derecho a la no discriminación, junto con la igualdad, ocupan un lugar fundamental en las normas sobre derechos humanos, ya que todos los derechos humanos (civiles, políticos, económicos, sociales y culturales) deben llevarse a la práctica por todo el mundo sin discriminación alguna y en total igualdad (Özden , 2011, p. 2). En definitiva, es fundamental que la aparente transparencia de algoritmos sesgados no sea tomada para disfrazar de justas decisiones automatizadas cuyos efectos son discriminatorios.

### *1.2.2 Decisiones desconocidas por el individuo*

Facebook realizó un experimento con 680.000 usuarios para determinar si las publicaciones que aparecían en su muro podían alterar su estado de ánimo. Se clasificaron diferentes tipos de publicaciones entre positivas y negativas con la ayuda de un algoritmo, repartiendo un tipo y otro entre los usuarios de la muestra. Este experimento mostró que aquellos usuarios

que habían recibido menos publicaciones alegres hicieron más publicaciones negativas y pesimistas, mientras que el grupo expuesto a mensajes positivos mostró un patrón optimista. O'Neill (2017) concluye que este experimento logra evidenciar el potencial de un algoritmo para influir en la emotividad de las personas y se pregunta qué sucedería si este mismo experimento se realizara un día que se celebren elecciones. Si bien no hay razón para creer que los científicos de Facebook están manipulando el sistema político, sí han demostrado el poder de la plataforma para influir en las acciones de los usuarios. Este ejemplo evidencia cómo opera la opacidad y falta de neutralidad de los algoritmos puede traer consecuencias desconocidas para el individuo que es objeto de escrutinio. Por otro lado, el caso del algoritmo de Google se asemeja al de Facebook, las personas creen que los resultados de búsqueda son rigurosos e imparciales, pero lo cierto es que es el algoritmo es el que define qué resultados van de primero, lo que pone de presente su potencial de ser manipulado (p. 170-180).

Análogamente, en el ámbito de las elecciones, cabe preguntarse por el marketing orientado al consumidor o *micro-targeting*, pues esta ofrece a los políticos nuevas vías para decir a grupos concretos de votantes justo lo que quieren saber. Lo mismo sucede con la difusión de noticias falsas a través del *micro-targeting* que suelen tener por objeto la viralización en redes sociales para alentar la movilización política. Esta estrategia funciona segmentando el contenido a través de publicaciones que solo el receptor puede ver. Campañas políticas como redes sociales, tienden a segmentar cada vez más el perfil de su público y, con la generalización de esta tendencia, cada vez es más difícil acceder al tipo de anuncios que llegan a las otras personas, ya que los sistemas asocian cada votante con información acumulada sobre sus historiales de compra, direcciones, números de teléfono, etc. Esta asimetría de la información impide que los hechos sean controvertidos. En definitiva, *el big data* permite que los individuos caigan en la falsa creencia de que los anuncios que ven en redes sociales son neutrales pues desconocen que son los algoritmos los que operan segmentando la información a partir del perfil del ciudadano.

### *1.2.3 Decisiones con efectos jurídicos para el individuo*

En los casos anteriores, se manifiestan riesgos para derechos fundamentales derivados de la opacidad y falta de neutralidad de los algoritmos, pero ninguno de estos tiene efectos jurídicos sobre las personas en el entendido de que no crea obligaciones para las personas o grupos que son objeto de análisis. La vigilancia masiva es uno de los casos que materializa esta problemática. Como se mencionó en el capítulo anterior, los atentados terroristas del 11 de septiembre de 2001 en Estados Unidos, los del 11 de marzo de 2004 en Madrid y los del 7 de julio en Londres dieron lugar a la ampliación de servicios policiales y de seguridad para la prevención del delito de terrorismo, tanto en Estados Unidos como en la Unión Europea.

Con ocasión de los atentados terroristas en Madrid y Londres, la Unión Europea promulgó la directiva de Retención de datos (2006/24/CE), la cual impondría a las empresas de telecomunicaciones la obligación de conservar los datos relacionados con registros de llamadas, acceso a internet, correo electrónico y telefonía por internet, con la finalidad de prevenir actos terroristas. En el 2014, el Tribunal de Justicia de la Unión Europea, en la sentencia C-293/12, estableció que dicha directiva vulneraba los derechos fundamentales, especialmente a la privacidad y *habeas data*, de la población europea; con respecto a la vigilancia masiva que suponía materializar las directrices que imponía la norma en cuestión, estableció que esta habría sido generalizada e indiscriminada y que la vigilancia solo se justifica ante la sospecha de un delito en concreto para una persona en concreto y por mandato de una entidad judicial con observancia del debido proceso (Betuzy, Coinu y Demuro, 2019, p. 259) .

Como se han mencionado, los problemas trascienden la privacidad. La extensión de las funciones policiales tradicionales dio lugar a la vigilancia e intercepción de los ciudadanos sin autorización judicial previa. En Estados Unidos, por ejemplo, las fuerzas del orden público (FBI, NSA, CIA, Fuerzas Militares) comparten sus bases de datos, las cuales contienen los datos de tráfico de los ciudadanos, a partir de “Centros de Fusión”. Esta agregación de datos de varias agencias permite a las fuerzas del orden público predecir o señalar a las personas como sospechosas o como objeto de investigación, búsqueda o detención según los criterios establecidos por la agencia. Este método de investigación puede

conducir a graves errores como los que se mencionan a continuación (Crawford y Schultz, 2014, p. 104).

La policía del estado de Maryland aprovechó su acceso a los centros de fusión para vigilar a grupos de derechos humanos, activistas por la paz y opositores a la pena de muerte durante un período de diecinueve meses. Debido a la labor de vigilancia, cincuenta y tres activistas políticos finalmente fueron clasificados como "terroristas" en los Centros de Fusión, incluidas dos monjas católicas y un candidato demócrata para a un puesto de elección local. El Centro de fusión compartió estas clasificaciones erróneas con las autoridades federales antidrogas, las bases de datos policiales y la Administración de Seguridad Nacional, todo ello sin darles a los inocentes la oportunidad de conocer, y mucho menos corregir, el registro (Crawford y Schultz, 2014, p. 104).

Asimismo, la Unión Americana por las Libertades Civiles (ACLU) expidió un informe denunciando el programa de vigilancia del Departamento de Policía de Nueva York cuya finalidad consistía en identificar posibles prácticas terroristas y de radicalización entre comunidades musulmanas y judías del Estado de Nueva York. El sistema de vigilancia tendría como finalidad generar reportes en las bases de datos de las agencias de inteligencia sobre aquellas personas que los algoritmos segmentan como peligrosas. La supuesta justificación de esta vigilancia inconstitucionales evidencia en un informe de la División de Inteligencia de NYPD de 2007 titulado "Radicalización en el oeste: una amenaza doméstica" (p. 1). El informe afirma que el programa de vigilancia tiene como finalidad rastrear el supuesto proceso de radicalización mediante el cual las personas se convierten en terroristas, pero los criterios usados para identificar dicho proceso eran tan amplios que parecían tratar con sospecha a cualquiera que se identifique como musulmán, comparta creencias o participe en prácticas religiosas islámicas.

El *big data* permite rastrear individuos que cumplan con el perfil diseñado por Departamentos de Policía, Fuerzas Militares o Agencias de Inteligencia. Estos perfiles se crean a partir de datos a los que se les asigna un valor. El problema surge cuando se trata de hallar la fórmula o programar un algoritmo para definir un valor tan abstracto como la potencialidad de ser

terrorista. La definición de estas características es completamente subjetiva y, como se evidencia en la vigilancia masiva, puede ser completamente arbitraria y generar consecuencias jurídicas para el individuo. Quienes son reportados erróneamente como potenciales terroristas en bases de datos de agencias de inteligencia y Fuerzas Militares con base en su registro digital, difícilmente pueden desprenderse de dicha etiqueta por parte del gobierno, lo que puede derivar en una investigación penal o sanciones civiles en contra del individuo (Hundt, 2014).

Si una persona quisiera saber qué categoría o perfil que le es aplicado o le resulta aplicable o qué lógica utiliza el algoritmo para llegar a sus conclusiones, podría encontrarse con varios obstáculos. A diferencia de los datos personales, los perfiles no tienen un estatus legal claro, no son datos personales, son el resultado de la aplicación de un algoritmo que puede estar protegido bajo derechos de propiedad intelectual o secreto empresarial, por lo cual, conocer la lógica con la que este opera es difícil. Los perfiles que se aplican a una persona porque sus datos coinciden con el perfil, a menudo se generan al extraer datos de otras personas. Para obtener acceso a este perfil, se tendría que alegar que cuando el algoritmo define que una persona pertenece a una categoría, esta información se convierte en un dato personal. Y, por último, si bien existe una norma en el ámbito comunitario que prevé la toma de decisiones automáticas con base en la creación de perfiles, si la persona no tiene conocimiento de ser sujeto de este tipo de decisiones, no podría ejercer este derecho (Hildebrandt, 2008, p. 12).

Si los ciudadanos no pueden ser protegidos ante el uso indebido de sus datos por parte del gobierno o las empresas, es como si perdieran su estatus de titulares de derechos y se convirtieran simplemente en grupos estadísticamente definidos, es decir, en perfiles o segmentos. Es por esto que la lucha por la privacidad necesariamente hace énfasis sobre la segmentación (Hundt, 2014). Pero, lastimosamente, los controles a la privacidad sobre los algoritmos, dejan de lado los problemas principales de la clasificación y segmentación por parte del *big data* (Dwork y Mulligan, 2013). En conclusión, el resultado del análisis de datos, es bastante problemático en tanto puede tener consecuencias que trascienden el ámbito de la privacidad. Es decir, los problemas del *big data* en relación con la creación de perfiles empiezan con la privacidad y la protección de datos, pero no se acaban allí. La interpretación

es central en el análisis de datos y, con independencia de la magnitud de la base de datos, los análisis están sujetos a limitaciones y sesgos debido a que pueden incluir datos erróneos, prejuicios, juicios de valor que acarrean consecuencias jurídicas desfavorables para el individuo y sin que exista publicidad sobre la forma en que se programa dicho algoritmo para que tome estas decisiones (O'Neill, 2017, p. 20).

## *3.3 Los efectos de los algoritmos en la autonomía y la democracia*

A continuación, se enunciarán cuáles son los posibles riesgos del uso de algoritmos para la creación de perfiles y la consecuente afectación de valores tales como la autonomía de los individuos y la democracia deliberativa, los cuales se analizan en el mismo aparte debido a la necesaria relación entre la autonomía y el ejercicio deliberativo. Posteriormente, se mencionan los posibles efectos de los algoritmos en un plano colectivo en relación con la creación de sesgos de confirmación y su intervención en la formación de la opinión pública. Estos problemas, si bien están relacionados también con la falta de transparencia del algoritmo, se analizan en un aparte diferente al 3.2 solo para efectos de orden.

### *3.3.1 La limitación a la autonomía*

Para Hildebrandt (2008) el problema para la autonomía, que presupone el mantenimiento de una libertad positiva y negativa, es la asimetría en el acceso efectivo al conocimiento entre el creador del perfil y la persona a la que se le aplica. Esta segunda, no conoce que se le está aplicando un perfil y, por ende, desconoce sus efectos, o, conociendo la existencia del perfil, desconoce cuál es la lógica de funcionamiento del algoritmo que los crea. En consecuencia, la opacidad de los algoritmos puede conducir a lo que se conoce como la trampa de la autonomía, es decir, precisamente porque una persona no es consciente de los perfiles que se le aplican, puede ser sugestionada para actuar de una manera que no hubiera diferente a cómo actuaría si conociera esta circunstancia. La creación de perfiles pone en riesgo la autonomía del individuo, que está relacionada con la posibilidad de una reflexión deliberada sobre nuestras posibilidades de acción, toda vez que, para ejercerla, es necesario tener acceso al conocimiento que determina las decisiones que se toman.

Hildebrandt (2008, p. 10) propone el siguiente ejemplo: el comportamiento en línea de un sujeto se recolecta y se combina con un perfil grupal que predice que la probabilidad de que sea un fumador que esté a punto de dejar de fumar es del 67%. Un segundo perfil predice que, si a ese mismo sujeto le ofrecen cigarrillos gratis junto con sus compras en línea y, adicionalmente, recibe noticias sobre la reducción de la demencia en fumadores, tiene un 80% de posibilidades de no dejar de fumar. Este conocimiento puede haber sido generado por compañías tabacaleras y puede ser usado para influir en el comportamiento.

Autores como Hildebrandt (2008) argumentan que la creación y aplicación de perfiles a los individuos suponen una vulneración para la libertad, que puede entenderse en un sentido positivo y uno negativo. La autora entiende la libertad positiva —libertad para— como aquella que permite participar en los procesos públicos de toma de decisiones o la libertad de lograr los objetivos personales; y libertad negativa o libertad —libertad de— se refiere a la ausencia de interferencias irrazonables impuestas a una persona para ejercer su voluntad. En ese orden de ideas, la autora argumenta que la elaboración de perfiles puede poner en peligro la combinación intrincada entre la libertad negativa y positiva cada vez que (1) las personas creen que no existe vulneración alguna a su esfera íntima, pero de hecho son observados por algoritmos que rastrean el comportamiento de los individuos en línea; y (2) cuando las personas creen que toman decisiones basadas en una representación de lo que está sucediendo, mientras que de hecho desconocen si están siendo objeto de perfilamiento y su lógica por parte de agentes privados y gubernamentales (Hildebrandt, 2008, p. 8).

En definitiva, se entiende que hay una afectación a la libertad en tanto el proceso de toma de decisiones del individuo se encuentra sugestionado por un tercero sin que el sujeto que toma la decisión conozca esta circunstancia. Esto pone en riesgo el ejercicio de la autonomía, que está relacionada con la posibilidad de una reflexión deliberada sobre nuestras posibilidades de acción, para lo cual es necesario tener acceso al conocimiento que determina las decisiones que se toman. En ese sentido, la creación y aplicación de perfiles no se compara con el uso de la retórica, no apelan a la razón del individuo, sino que tratan de sugestionarlo para que su comportamiento sea rentable. No hay certeza de que la persona actúe de conformidad a

esa predicción, pero su autonomía afecta mientras se desconozcan los fundamentos fácticos que la llevan a optar por una decisión u otra (Hildebrandt, 2008, p. 10).

### *3.3.2 Discusión sobre el papel de los algoritmos en la democracia y opinión pública: construcción o destrucción*

El proceso de creación de propaganda electoral personalizada en el que los algoritmos agrupan a la población de votantes en perfiles según las características psicológicas con la finalidad ulterior de desarrollar la propaganda electoral según el perfil de cada sujeto y pronosticar cómo el elector se comporta ante esta, es el ejemplo del empleo de algoritmos en el contexto de la sugestión del comportamiento. En el contexto de las elecciones, la diferencia entre una campaña electoral común y una en la que se le suman herramientas como los algoritmos, radica en la posibilidad de influir en las decisiones a través de argumentos o juicios de valor que permitan tomar una decisión libremente, mientras que la minería de datos en el contexto electoral tiene por objetivo inducir al individuo a tomar tales decisiones. En este último caso, el elemento de libertad en la toma de una decisión puede estar viciado por el uso de técnicas poco transparentes, que inducen al individuo a adoptar un determinado comportamiento o una determinada decisión, de manera inconsciente (Cotino, 2018, p. 140).

En este supuesto, las prácticas en cuestión, más que afectar la autonomía individual, afectan aspectos de la democracia como la posibilidad de deliberación. En el caso de Cambridge Analytica, el contenido de la publicidad era tan preciso y adaptado al perfil psicológico de su receptor, que su finalidad no podría ser otra que sugestionar el comportamiento del elector a quien estuviera dirigido. El problema no radica solamente en el uso abusivo de datos personales, sino también en la influencia que esto puede generar en el ejercicio de deliberación por parte del elector en el ámbito de la democracia. Para explicar brevemente cómo las herramientas persuasivas dirigidas al elector pueden afectar el ideal democrático, primero será necesario definir qué se entiende por democracia desde la filosofía política. Jeremy Waldron (2012) entiende la democracia como el gobierno del pueblo, el cual supone que, en oposición a las oligarquías, monarquías o dictaduras, los asuntos políticos deben ser confiados al pueblo. Para Waldron, el pueblo debe ser entendido desde una perspectiva individualista, es decir, no como un ente con identidad propia del cual se puede inferir su

voluntad, sino como la voluntad de millones de individuos y el resultado político determinado por la expresión de millones de voluntades. Así como se entiende que los sujetos son plenamente autónomos para contratar, contraer derechos y obligaciones y, en general, decidir sobre su proyecto de vida, se considera que todos los ciudadanos mayores de edad son autónomos y plenamente capaces para intervenir y contribuir en el proceso de toma de decisiones políticas, razón por la cual se busca otorgar tanto peso como sea posible al punto de vista de cada individuo, pero a ninguno más que a los demás (Waldron, 2012, pp. 187-203). Robert B. Talisse (2012) considera que, además del voto, se contribuye en el proceso de toma de decisiones políticas a partir de la deliberación, principio que fundamenta la democracia deliberativa y que no es más que cualquier actividad que tenga el objetivo de brindar consideraciones racionales para tomar una decisión (p. 210).

La deliberación en cualquiera de sus acepciones, presupone una decisión libre e informada por parte de los ciudadanos, cualquiera sea la aproximación que se tome. La democracia deliberativa concibe la deliberación como el elemento esencial que conlleva a la vinculación colectiva de las decisiones democráticas, lo que se traduce en la legitimación del sistema. Phillip Petit, considera que la deliberación requiere que los ciudadanos tomen decisiones libres, es decir, que no se encuentren sujetas a la interferencia arbitraria de terceros (p. 212). En una Estado democrático en el cual la información personal de los ciudadanos puede ser utilizada para incidir en su comportamiento mediante el uso de herramientas altamente persuasivas, al margen de su capacidad de control o conocimiento, saltan las alarmas por la posible manipulación de su voluntad y capacidad de decidir, lo cuál constituye la más ostensible afectación a la autonomía que fundamenta la participación de los ciudadanos en la toma de decisiones políticas y a la legitimidad misma del sistema (Arenas, 2019, p. 343).

Hasta el momento, se han analizado los efectos de los algoritmos en la formulación de decisiones por parte del individuo. Pero no hay que perder de vista el efecto de los algoritmos puede evidenciarse en el plano colectivo en relación con la formulación de opiniones. Cuando nos preguntamos cuál es el efecto del big data sobre la opinión pública. Existe la creencia de que el internet conduce a una sociedad más informada, pero lo cierto es que la capacidad de procesamiento de información de los humanos es limitada y depende del nivel educativo de la persona. Asimismo, los motores de búsqueda operan sistemáticamente para favorecer a

algunos sitios web y si bien Internet ofrece fuentes alternativas de información, la mayoría de las personas no se preocupan por indagar sobre la veracidad de la información que reciben (de Angelis, 2016, p. 10).

Es difícil establecer cuál es el verdadero efecto del big data en la construcción de la opinión pública, pero no hay duda de que permite construir una realidad individualizada. Los algoritmos de los motores de búsqueda y de redes sociales no son neutrales, estos crean la tendencia de compartir información de usuarios que presentan un perfil similar al propio, lo cual tiene como efecto inducir a la opinión pública en errores y favorecer la difusión de noticias falsas en públicos polarizados. Adicionalmente, las personas no necesariamente se percatan por cuestionar la información que consumen, especialmente cuando confirma sus creencias anteriores. Cuanto esto ocurre, caen en los que los psicólogos llaman sesgo de confirmación (González, 2018, p. 296; O'Neill, 2017, p. 180).

Los algoritmos de redes sociales y motores de búsqueda le muestran al individuo contenidos con los que podría estar potencialmente de acuerdo y desecha aquellos que pueden generarle conflicto, ignorando así su autonomía sobre la información que recibe. Este modo de difundir información es especialmente problemático cuando se trata de noticias, ya que permite que las noticias verdaderas como aquellas que son manifiestamente falsas sean compartidas en igualdad de condiciones por el algoritmo. "Este fenómeno ha llevado a establecer el potencial de lo que ya se conoce como *posverdad*, que ampara lo que podríamos llamar la certeza de las mentiras, y que ha ganado la posición de palabra del año 2016 otorgada por el Oxford Dictionary" (Colmenarejo, 2017, p. 57).

Autores como Cotino (2018, p. 140) han discutido cuál el efecto del filtrado y la ceración de contenidos para la democracia deliberativa. Desde una perspectiva pesimista, se ha entendido que la personalización de contenidos conlleva a una limitación del mercado de las ideas que es tan importante en una sociedad libre toda vez que refuerza las posiciones particulares, sin apertura ni compromiso con lo diferente, es decir, limita el ejercicio deliberativo en el ámbito de la democracia. El autor sostiene que la personalización de contenidos conlleva la desaparición del foro público. "En la red y con los sistemas de personalización se crean "enclaves deliberativos" que no hacen, sino que reforzar las posiciones individuales,

contribuyendo a extremar y polarizar la esfera pública" (Sustein, 2001, p. 67 y 71 como se cita en Cotino, 2018, p. 140). Por el contrario, desde la perspectiva optimista, se considera que Internet amplia la esfera pública al permitir que la persona conozca diversas posturas y posiciones a las que, en su vida cotidiana, no tendría acceso.

Con independencia de si se adopta una postura pesimista u optimista, no se puede dejar de lado la problemática resultante de la difusión de fake news, que son la más clara demostración del mal funcionamiento de los algoritmos en redes sociales y motores de búsqueda. En efecto, "en una democracia, la generación de noticias falsas representa claramente la desvirtuación de un valor central para la creación de una opinión pública libre y correctamente informada que constituye la base para una participación responsable en la formación de la opinión y preferencias políticas de los ciudadanos" (González, 2018, p. 289).

En definitiva, la creación y aplicación de perfiles puede tener efectos para la democracia en dos ámbitos: en un ámbito individual, cuando la aplicación de perfiles es desconocida por el individuo, cuyas decisiones se ven influenciadas por algoritmos; y en un plano colectivo, cuando los algoritmos de filtrado promueven la creación de sesgos de confirmación y la propagación de noticias falsas.

# 4. DEFICIENCIAS DE LA REGULACIÓN VIGENTE: EL CASO COLOMBIANO

Este capítulo tiene como finalidad realizar un análisis jurídico sobre la pertinencia de las normas colombianas en materia de datos personales para dar solución a las problemáticas planteadas en el capítulo anterior en torno a la privacidad y el uso de algoritmos. Para tales efectos, se discutirá qué autoridad debe expedir el marco normativo, para luego determinar si la regulación doméstica o interna de cada estado es suficiente para afrontar las problemáticas planteadas. En segundo lugar, se expondrán las dificultades de la legislación actual y diversos argumentos doctrinales que ponen de manifiesto la insuficiencia del régimen colombiano de protección de datos personales para abordar distintos aspectos que surgen del uso de algoritmos,de *big data* e inteligencia artificial y se plantearán algunas soluciones propuestas por la doctrina y organismos de cooperación internacional como la Unión Europea para abordar el problema en torno a la protección de datos. Por último, se propondrán soluciones y aproximaciones desde la Organización para a Cooperación y el Desarrollo Económicos, de ahora en adelante, OCDE, y la Unión Europea para regular el uso y aplicación responsable de algoritmos, de *big data* e inteligencia artificial, que sea respetuosa de los derechos y libertades básicas de las personas.

Para delimitar el objeto de estudio es necesario señalar que las problemáticas que se abordarán son dos: aquellas relacionadas con la privacidad y la protección de datos personales y, aquellas que se derivan de la naturaleza y el diseño de las tecnología de procesamiento de información. Para ello, se debe establecer qué normas componen el régimen colombiano de protección de datos personales. Se trata de un compendio de normas cuyo fundamento constitucional se encuentra en el art. 15 de la Constitución Política que consagra el derecho fundamental de habeas data como el derecho de toda persona a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. La Ley Estatutaria 1266 de 2008, reglamentada por el Decreto 2952 de 2010, desarrolla el núcleo esencial de este derecho frente a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. La Ley estatutaria 1581 de 2012, reglamentada por el Decreto 1377 de 2013, regula de manera general el tratamiento de datos personales y los principios generales que

rigen el tratamiento de datos. Asimismo, la sentencia C-748 de 2011 conforma este régimen al evaluar la constitucionalidad de esta última ley (Newman y Ángel, 2019, p. 45; Martínez, 2019, p. 9). Para efectos de el análisis actual, nos centraremos en la Ley Ley estatutaria 1581 de 2012, debido a que esta es la norma general.

La autoridad competente de velar por el cumplimiento de las disposiciones de este régimen según el art. 21 de la Ley 1581 de 2012 es la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio (de ahora en adelante, SIC), la cual debe ejercer funciones regulatorias, de control y vigilancia y sancionatorias.

En cuanto a la segunda problemática que nos compete, esto es, la regulación que prevea y mitigue los riesgos derivados del uso de algoritmos de *big data* e inteligencia artificial, en Colombia es inexistente a nivel constitucional, legal o jurisprudencial que establezcan un marco regulatorio orientado a promover el uso responsable y ético de algoritmos de *big data* o inteligencia artificial. A continuación, se analizará la necesidad de promover normas de carácter internacional que permitan regular estas problemáticas de manera unificada.

### *4.1. Alcance de las regulaciones domésticas para enfrentar una problemática global*

El ámbito de aplicación de la ley colombiana en materia de datos personales es limitado. Los nuevos escenarios tecnológicos han demostrado que la protección a la vida privada, a los datos personales, a la igualdad y a otros derechos fundamentales no son problemáticas que se circunscriben a un solo territorio ya que su alcance trasciende las fronteras de los Estados en virtud de la circulación internacional de datos personales y su tratamiento por parte de empresas excluidas del ámbito de aplicación de la ley.

De acuerdo con el artículo 2 de la Ley 1581 de 2012, su régimen de protección de datos es aplicable al tratamiento de datos personales cuando sea efectuado en territorio colombiano, o cuando al responsable o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

La Superintendencia de Industria y Comercio entendía que el régimen colombiano de protección de datos personales no le era aplicable a plataformas de redes sociales pues el tratamiento no se realizaba dentro del territorio colombiano (Concepto 14-218349–00003-0000 del 24 de noviembre de 2014). No obstante, a partir del Concepto 14-218349–4- 0 del 3 de marzo de 2016, la SIC añadió un criterio adicional al ámbito de aplicación de la ley al considerar que la normatividad también debía ser aplicable al tratamiento de datos personales efectuado por proveedores de servicios de redes sociales establecidos fuera del país, a través de un "medio" situado en territorio colombiano (Ángel y Newman, 2019, p. 76).

La SIC no mencionó expresamente qué se entendería por "medio". Algunos doctrinantes han entendido que la expresión "medio" hace referencia a las cookies, pero si se entiende de esta manera, se excluirían otras fuentes mediante las cuales las plataformas de redes sociales y todo tipo de empresas que operan mediante servidores en la web obtienen la información [12](Ángel y Newman, 2019, p. 35 y pp. 76-77).

Las normas nacionales colombianas en materia de datos personales son insuficientes en tanto su ámbito de aplicación se condiciona a la ubicación del encargado del tratamiento y no a la ubicación del titular de los datos, lo cual puede derivar en la desprotección de los datos de los titulares si las normas de protección aplicables a los responsables del tratamiento cuentan con un menor estándar de protección. Lo mismo pasaría en el escenario de las transferencias internacionales de datos, esto es, la importación o exportación de información de un país a otro, si el país receptor cuenta con un nivel deficiente de protección de datos (Remolina, 2010, p. 495).

En relación con las transferencias nacionales, para 1990, la Organización de Naciones Unidas adoptó los *Principios rectores para la reglamentación de los ficheros computadorizados de datos personales*, reglamentando el principio de flujo de datos a través de las fronteras según el cual "cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información

[12] Por ejemplo: la información provista directamente por el titular, o mediante una compraventa de datos, mediante transferencias de socios estratégicos - empresas de marketing que proporcionan servicios publicitarios y de investigación, terceros que prestan servicios en nombre de la empresa, otras plataformas sincronizadas, etc.- (Ángel y Newman, 2019, p. 35)

debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos" (Remolina, 2010, p. 498).

El flujo global de datos pone a pruebas las normas y aproximaciones nacionales para la protección de datos personales. Las personas pueden conectarse a Internet desde cualquier parte del mundo, y los datos almacenados en la "nube" se pueden respaldar en múltiples ubicaciones (ubicaciones que solo conoce el operador de la nube), volviendo cada vez más complejas cuestiones relacionadas con la jurisdicción, vigilancia y control, y seguridad jurídica de la protección de datos. Optar por una regulación exclusivamente nacional o, incluso, regional, no resuelve ni provee la protección de datos personales que los individuos esperarían en el ámbito de una economía global (OCDE, 2013, p. 101).

El ámbito de aplicación de la ley y el flujo transfronterizo de datos son problemáticas que ponen de presente la necesidad de unificar normas en materia de protección de datos personales a través de instrumentos internacionales que cuenten con mecanismos internacionales de verificación, debido a 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. Lograr un estándar alto de protección que fuese común a todos los Estados permitiría aumentar la competitividad, generar confianza en la inversión extranjera, facilitar la celebración de negocios, y promover la libre circulación de los datos (Martínez, 2019, p. 13).

La importancia de la unificación normativa no solo es evidente por sus bondades, sino para evitar la vulneración de lo derechos de los titulares de los datos. El caso de Cambridge Analytica es solo uno de los supuestos en los que se demuestra cómo se hizo un tratamiento abusivo de los datos personales de los ciudadanos estadounidenses por parte de una empresa inglesa 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, lo cual evidencia la facilidad con la que las normas de protección de datos pueden incumplirse desconociendo completamente fronteras y jurisdicciones (Martínez, 2019, p. 13). Si bien un enfoque global sería la opción más adecuada, es claro que no está exenta de desafíos prácticos. or más garantista que sea la

legislación nacional, por sí sola no puede abarcar una problemática que se manifiesta en la virtualidad, rebasando las jurisdicciones estatales.

Ahora bien, la regulación de las consecuencias del uso de algoritmos de *big data* e inteligencia artificial, ya sea porque se trata de tecnologías que aún está en desarrollo y cuyos potencial riesgos y beneficios están por descubrirse, se caracteriza por su escasez en el ámbito internacional y su inexistencia en el nacional. Ahora bien, existen normas de *soft law* expedidas por organizaciones de cooperación internacional, tales como la Recomendación del Consejo de la OCDE sobre Inteligencia Artificial de 2019 o el Libro Blanco sobre Inteligencia Artificial de la Comisión Europea de 2020, las cuales no tienen fuerza vinculante pues su función es establecer, a modo de recomendación, estándares para ser adoptados en el derecho interno de los Estados. Pero es claro que estos mecanismos no son suficientes para afrontar las problemáticas que derivan del diseño de los algoritmos pues su incorporación es facultativa. a Recomendación de la OCDE hace un llamado a la regulación y cooperación global con la doble finalidad de promover los beneficios de esta tecnología en relación a la innovación y productividad en sectores como las finanzas, salud, transporte e impulsar la economía de aquellos países cuyas mercados se encuentran en desventaja con respecto al mercado global, y plantear los desafíos del uso de algoritmos en relación a las problemáticas que surgen de la opacidad y sesgos implícitos, como las implicaciones para la igualdad, la democracia y los derechos humanos (OCDE, 2019).

La interconectividad de aparatos electrónicos inteligentes, la disponibilidad de cantidades masivas de datos, la accesibilidad a servidores que facilitan el registro y almacenamiento de datos que crecen exponencialmente y el desarrollo de métodos estadísticos de aprendizaje automático, son las circunstancias actuales que refuerzan la escalabilidad y la progresiva importancia que han ido adquiriendo los algoritmos en la sociedad. Las consecuencias para la democracia y los derechos humanos fueron enunciadas en el capítulo anterior, y la posible materialización de los mencionados riesgos es razón suficiente para abogar por la adopción de principio y parámetros de transparencia y responsabilidad a nivel global (Colmenarejo, 2017, p. 85).

La adopción de estos parámetros y principios desde una aproximación global, debe realizarse por organizaciones que tengan influencia a nivel mundial, esto es, la Organización de Naciones Unidas. Esta debería tomar en consideración cuestiones como a *dónde queremos llegar* y cómo se pueden adecuar las nuevas tecnologías a los objetivos que persigue la humanidad, lo que implicaría orientar el discurso hacia el bien común. En la actualidad, ya existe un consenso sobre las finalidades que persigue la humanidad en el futuro: *Our common future* es un informe aprobado por la Asamblea General de las Naciones Unidas en 1985 en el que se recogen los primeros objetivos de desarrollo consensuados mundialmente bajo la denominación de desarrollo sostenible, el cual exige que cualquier forma de desarrollo debe medir su impacto en las generaciones futuras. En el 2015, se aprobaron los *Objetivos de desarrollo sostenible* con la finalidad de erradicar la pobreza, las desigualdades y promover el desarrollo de los pueblos y la protección del medio ambiente. El desarrollo de esta tecnología debe ir en línea con estos objetivos, lo cual solo es posible a partir de una regulación global (Colmenarejo, 2017, pp. 85-86).

### *4.2. Ausencias, dificultades de la normatividad colombiana y propuestas generales para enfrentar estas falencias*

En este aparte se realizarán, en primer lugar, un análisis respecto de aquellos temas que no son contemplados en la legislación actual de protección de datos personales y que son necesarios para afrontar las problemáticas sobre privacidad expuestas en el capítulo anterior y, adicionalmente, se expondrá la manera en que estos aspectos han sido regulados en la Unión Europea. Posteriormente, ante la ausencia de normatividad que regule el uso de algoritmos en Colombia, se expondrán dos aproximaciones para abordar los problemas que surgen de la opacidad y los sesgos de los algoritmos propuestas por organizaciones de cooperación internacional como la OCDE y la Unión Europea y una tercera aproximación doctrinal.

A continuación, se realizará un listado de los asuntos que no son contemplados por la legislación con fundamento en la investigación titulada *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital* realizado

por Vivian Newman y María Paula Ángel para la ONG DeJusticia, y cómo estas nuevas modalidades de tratamiento de datos personales han sido abordadas por otras legislaciones.

#### *4.2.1. Predicciones e inferencias de datos sensibles*

Los datos sensibles son definidos en el art. 5 de la Ley 1581 de 2012 de la siguiente manera:

> Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Ángel y Newman (2019) indican que esta definición no especifica el medio mediante el cual se obtiene el dato, es decir, si son entregados directamente por el titular o por otra fuente, por lo cual, si un dato sensible es inferido de otros datos personales, su tratamiento estaría prohibido salvo si concurre alguna de las excepciones del art. 6 de la Ley 1581 de 2012[13]. Pero este artículo ni la definición de datos personales en Colombia consideran como sensibles aquellos datos que, no siendo sensibles en principio (como un historial de compras), en conjunto con otros permiten inferir datos sensibles. Aquellos datos que en principio no son considerados como sensibles también permitirían revelar información que afectaría la intimidad del titular, pero a la luz de la normatividad colombiana no estarían sujetos a la misma protección (Ángel y Newman, 2019, pp. 47-48).

Ahora bien, La *Ley de privacidad del consumidor de California*, en el literal O, sección 1787, contempla dentro de la definición de dato personal las inferencias extraídas de cualquier tipo

[13] A) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; B) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado; C) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad; D) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; E) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

de información personal para crear un perfil sobre un consumidor que refleje sus preferencias, características, tendencias psicológicas, predisposiciones, comportamientos, actitudes, datos biométricos, psicométricos, geolocalización y el historial de navegación por internet. La legislación colombiana podría tomar esta norma como referente para evitar la desprotección de datos sensibles que se deducen de otros que no lo son.

Asimismo, el art. 14 del RGDP establece requisitos adicionales y detallados de transparencia cuando la información no fue entregada voluntariamente por el titular, tales como la especificación de los fines del tratamiento, las categorías de datos personales a tratar y el destino de dichos datos (es decir, si los datos serán objeto de transferencias internacionales), si hay un interés legítimo para tratar los datos cuando se trate de datos sensibles, la fuente de la cual proceden los datos, la existencia de decisiones automatizadas, etc. En definitiva, la legislación debe establecer reglas estrictas para el tratamiento de los datos sensibles inferidos y exigencias adicionales al requerir el consentimiento para inferir información nueva del titular debido a la importancia del tipo de datos que se infieren y la estrecha relación con el derecho a la intimidad.

#### *4.2.2. La falta de claridad sobre direcciones IP y otros identificadores en línea como cookies e identificadores de radiofrecuencia*

Los datos personales son definidos en el art. 3 de la Ley 1581 de 2012 como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables". Esta definición no menciona ejemplos y, por lo tanto, no se refiere expresamente a las direcciones IP, que son números seriales de cada dispositivo que intenta conectarse a internet, el cual es único para este. En otras legislaciones, como en el art. 4 del GDPR de la Unión Europea, se han incluido estos datos dentro de la definición de datos personales debido a que estos permiten determinar la identidad de una persona física de manera directa o indirecta. De manera indirecta, una persona puede ser identificada al asociar el identificador en línea de su dispositivo con otros datos recibidos por los servidores de internet. Asimismo, los datos asociados a las direcciones IP, que en principio no son atribuibles a una persona sino a una identificación numérica, como el historial en motores de búsqueda, el rastro digital, etc.  por lo que no serían datos personales, pero a partir de

algoritmos, es posible vincular esta información a personas determinables (Ángel y Newman, 2019, pp. 48-51).

Las direcciones IP, cookies y datos recolectados de identificadores en línea no son considerados datos personales salvo que cumplan con las condiciones del Concepto Radicado No. 16-172268 del 9 de agosto de 2016 de la Superintendencia de Industria y comercio, las cuales son:

> (i) Están referidos a aspectos exclusivos y propios de una persona natural, ii) permiten identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación; caso en el cual, el responsable deberá ceñirse por las normas sobre protección de datos vigentes en Colombia.

Como menciona el numeral ii), solo a partir del análisis de conjuntos de metadatos se puede saber si estos datos permiten identificar a una persona. Es decir, el reconocimiento de estos datos como datos personales se somete a un análisis *ex post*, en el cual solo se sabe si este conjunto de datos permiten identificar a una persona solo después de haber sido sometidos a tratamiento, lo cual es problemático para la garantía del consentimiento informado que exige que este debe ser anterior al tratamiento de los datos (González Guerrero, 2018, p. 225).

Ángel y Newman (2019) proponen que, como en otras legislaciones es claro que las direcciones IP permiten identificar a una persona, se podría interpretar que estos datos se encontrarían incluidos dentro de la clasificación de dato personal en Colombia. Sin embargo, hasta que no haya una norma clara al respecto, no habrá seguridad jurídica y quedaría al arbitrio del responsable del tratamiento considerarlo como un dato personal (p. 51).

#### *4.2.3. La creación de perfiles y las decisiones automatizadas*

La Corte Constitucional desde la sentencia T-414 de 1992 ya advertía que los perfiles son una especie de representación virtual de la persona a partir de sus datos, pero que puede tener significativas repercusiones en la persona real (Ángela y Newman, 2019, p. 62). Desde el capítulo anterior, se advirtió que estas repercusiones se materializan en riesgos tanto para los datos personales, como para la igualdad, la libertad de expresión, la autonomía, etc. Esto puede usarse para medir, clasificar y evaluar a las personas, y para tomar e informar decisiones sobre ellas que pueden o no ser automatizadas (Privacy International, 2018, p. 61). En la legislación colombiana, no existe norma que regule este supuesto a pesar de los graves riesgos que conlleva.

Al respecto, la legislación colombiana podría adoptar la ruta tomada por la Unión Europea en el GDPR en cuanto a la promoción de la transparencia en la construcción de perfiles. En el Considerando 60 del GDPR, se establece que "los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. (...). *Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración".* En ese orden de ideas, el art. 14 del GDPR que establece exigencias adicionales cuando los datos no fueron entregados voluntariamente al titular, obliga al responsable del tratamiento de los datos a informar al titular sobre la existencia de decisiones automatizadas, la elaboración de perfiles, y la lógica aplicada para tomar tal decisión, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado (Ángel y Newman, 2019, p. 64).

La legislación colombiana debe imponer restricciones y garantías en la toma de decisiones automatizadas y en la creación de perfiles. Sectores de la doctrina consideran que la aproximación más apropiada para regular estos como tratamiento de datos personales es consolidar el derecho a no ser objeto de estos cuando puedan tener consecuencias para las personas y afectar sus derechos. Para asegurar una mayor protección, es importante que el precepto normativo imponga una prohibición de someter a las personas a decisiones automatizadas y/o perfiles, salvo determinadas excepciones (Privacy International, 2018, p. 61).

En línea con dicho planteamiento, el art. 22 de GDPR consolida el derecho de los titulares de los datos a no ser objeto de una decisión basada únicamente en el tratamiento

automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar salvo que ésta sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento, que la decisión esté autorizada por la Unión europea y que contenga medidas adecuadas para proteger sus derechos, o que sea autorizada por el titular de los datos.

Adicionalmente, el RGDP otorga al titular la posibilidad de rechazar esta finalidad del tratamiento y, en caso de aceptarla, le permite obtener intervención humana por parte del responsable, expresar su punto de vista e impugnar la decisión (Ángel y Newman, 2019, p. 68).

#### *4.2.4. Contenidos personalizados*

En Colombia la regulación de contenidos personalizados no va más allá de considerarla como una finalidad del tratamiento de datos personales, por lo cual solo se exige que la finalidad sea legítima y sea informada al titular. Los contenidos personalizados se basan en la creación de perfiles y en la observación del comportamiento de las personas en el tiempo a través de sus búsquedas en internet para proporcionar publicidad adaptada a los intereses de la persona. Es de suma importancia que esta finalidad sea regulada para impedir invasiones ilegítimas en la vida privada de los titulares de datos, especialmente porque esta práctica suele ser desconocida por los titulares de los datos e involucra varios actores.

En el proceso de creación de contenidos intervienen los anunciantes y los proveedores de redes publicitarias, quienes instalan cookies, crean perfiles de los usuarios y promueven sus productos a partir de anuncios publicitarios. Como se establece en el considerando 58 del RGDP, el problema de la publicidad personalizada para la protección de datos personales consiste en que “la proliferación de actores y la complejidad tecnológica de la práctica hacen que sea difícil para el titular saber y entender si, por quién y con qué propósito se recopilan datos personales relacionados con él” (Ángel y Newman, 2019, pp. 65-66).

#### *4.2.5. Consentimiento previo, expreso e informado*

A diferencia de los supuestos anteriormente expuestos, el consentimiento previo constituye el núcleo del Régimen de protección de datos personales y el mecanismo que permite a los

titulares autorizar el tratamiento de sus datos personales. El art. 9 de la Ley 1581 exige que el consentimiento sea previo y que sea obtenido por cualquier medio de consulta posterior. El art. 7 del Decreto reglamentario 1377 de 2013 establece que el consentimiento se entiende otorgado mediante conductas inequívocas del titular que permiten concluir de forma razonable que se otorgó la autorización.

El problema con el consentimiento informado es que es completamente inocuo cuando se trata de páginas web, redes sociales y todo tipo de plataformas de internet debido a que el consentimiento suele ser otorgado a partir de términos y condiciones y, en consecuencia, no suelen ser leídas por su extensión y complejidad. Por su vaguedad, es difícil dimensionar las implicaciones de aceptarlas. Adicionalmente, no dan la oportunidad al titular de los datos de seleccionar cada tratamiento que desea aceptar porque estas son presentadas en bloque y condicionan la prestación del servicio a la aceptación de la totalidad de dichas políticas (Ángel y Newman, 2019, p. 71).

Este planteamiento permite cuestionar la utilidad de consentimiento previo para proteger efectivamente los datos personales, por lo cual se propone que la legislación colombiana siga la misma línea de regulación de la Unión Europea. En la Unión Europea se modificó la legislación en torno a la protección de datos personales para garantizar el cumplimiento efectivo del consentimiento para afrontar estos desafíos. El art. 7 del RGPD regula los requisitos para otorgar el consentimiento el cual, a diferencia del consentimiento colombiano, se define en el art. 4 como una manifestación inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Al respecto, el Grupo de Trabajo del Art. 29, que es el órgano consultivo independiente en materia de protección de datos personales en la Unión Europea, elaboró una guía para identificar cuando el consentimiento es válido. El órgano consultivo elaboró un informe titulado *Directrices sobre el consentimiento en virtud del Reglamento 2016/679*, el cual constituye una guía para determinar cuando se considera que consentimiento es libre, informado y es una manifestación inequívoca. El órgano consultivo entiende que el consentimiento es libre porque el titular tiene el control efectivo sobre sus datos, es decir, no se considera libre si esta no puede negarse o retirarlo en cualquier momento y sin perjuicio

alguno. Tampoco se considera libre si la ejecución de un contrato o la prestación de un servicio se supedita a otorgar el consentimiento sobre datos que no son esenciales para este fin (por ejemplo, si el acceso a una aplicación de edición de fotos se condiciona a tener prendido el GPS o el micrófono del dispositivo). Por último, tampoco es libre si las finalidades deben aceptarse en bloque, por lo tanto, la persona debe poder aceptar cada finalidad selectivamente (González Guerrero, 2018, p. 226).

Ahora bien, para que el consentimiento sea informado, se debe dar a conocer a la persona si está siendo objeto de decisiones automatizadas, si desea oponerse al *marketing* directo y los posibles riesgos por transferencias de datos a países que no cuenten con garantías suficientes de protección de datos. Por otro lado, se considera que el consentimiento es inequívoco si es un acto afirmativo y claro, y si el consentimiento puede distinguirse de otras acciones como usar el servicio ofrecido o hacer clic en el sitio web, es decir, este no puede ser un acto inferido sino expreso (González Guerrero, 2018, p. 227).

Por último, el grupo de trabajo del Art. 29 propone optar por el doble consentimiento cuando se trate de datos personales sensibles, cuando los datos sean objeto de transferencias internacionales o cuando se usen para la toma de decisiones automatizadas o en perfiles. El doble consentimiento consistiría en realizar una manifestación de aceptación y, adicionalmente, ingresar códigos de confirmación o ingresar a un enlace para aceptar nuevamente, por ejemplo (González Guerrero, 2018, p. 227).

En conclusión, es evidente como el régimen colombiano de protección de datos personales se encuentra desactualizado. Las disposiciones que contempla son inexistentes, como en el caso de los perfiles, decisiones automatizadas, inferencia de datos personales sensibles y publicidad personalizada, e insuficientes, como en el caso del consentimiento, para abordar las problemáticas actuales que se presentan en el contexto de internet y el uso de algoritmos.

### *4.3. Aproximaciones y consideraciones para elaborar un marco regulatorio de big data e inteligencia artificial*

Es claro que no existe regulación interna en Colombia sobre el uso de algoritmos de b*ig data* o inteligencia artificial. En 2019, Colombia, junto a otros 41 países adoptó la Recomendación

del Consejo de la OCDE sobre inteligencia artificial, la cual consta de una declaración de principios cuya finalidad es servir de guía a los gobiernos para que, en el diseño y la gestión de los sistemas de inteligencia artificial, prioricen los intereses de las personas, así como garantizar que quienes diseñen y gestionen sistemas de inteligencia artificial respondan de su correcto funcionamiento (OCDE, 2019). Los principios promulgados por la OCDE (2019), respaldados por la Unión Europea, son los siguientes:

i. La IA debe estar al servicio de las personas y del planeta, impulsando un crecimiento inclusivo, el desarrollo sostenible y el bienestar.

ii. Deben diseñarse de manera que respeten el Estado de derecho, los derechos humanos, los valores democráticos y la diversidad, e incorporar salvaguardias adecuadas —por ejemplo, permitiendo la intervención humana cuando sea necesario— con miras a garantizar una sociedad justa y equitativa.

iii. Deben estar presididos por la transparencia y una divulgación responsable a fin de garantizar que las personas sepan cuándo están interactuando con ellos y puedan oponerse a los resultados de esa interacción.

iv. Estos deben funcionar con robustez, de manera fiable y segura durante toda su vida útil, y los potenciales riesgos deberán evaluarse y gestionarse en todo momento.

v. Las organizaciones y las personas que desarrollen, desplieguen o gestionen sistemas de IA deberán responder de su correcto funcionamiento en consonancia con los principios precedentes.

En línea con estos principios, la Unión Europea creó una iniciativa de regulación de algoritmos cuya finalidad es promover el uso de estas tecnologías asegurando el respeto de los derechos humanos y mitigando sus riesgos. Se decidió exponer esta iniciativa debido a que se trata de una propuesta que desarrolla estos principios con medidas más concretas para realizar auditorías.

*Libro blanco de inteligencia artificial*

El Libro Blanco de inteligencia artificial es un documento emitido por la Comisión Europea en abril de 2020 con la finalidad de establecer una propuesta de regulación para mitigar los riesgos que se asocian al uso de algoritmos y al mismo tiempo promover el uso de estas tecnologías. La Comisión Europea señala que el uso de algoritmos representa diversas

ventajas, pero también puede conllevar a la producción de daños materiales como inmateriales. Los primeros hacen referencia a la producción de daños a la salud, propiedad o vida como consecuencia de falla en algoritmos incorporados en productos o servicios, por ejemplo, si un vehículo operado por algoritmos causa un accidente de tránsito. En cambio, los daños inmateriales son aquellos que se refieren a la vulneración de un derecho fundamental en razón de las características propias de la tecnología, como la opacidad, los sesgos implícitos y la falta de intervención humana. Para efectos de este estudio, solo nos centraremos en las soluciones propuestas para mitigar los daños inmateriales.

*i. Ámbito de aplicación del marco regulatorio*

La Comisión europea señala que la principal error es asumir que un marco regulatorio de inteligencia artificial deba aplicarse a todo producto o servicio que dependa de la inteligencia artificial, pero si lo que se quiere es promover el uso de la tecnología, se debe asegurar que esta política no caiga en el exceso de ser demasiado descriptiva para no crear cargas desproporcionadas en los particulares y poder abarcar nuevos desarrollos de la tecnología en el futuro. Por esta razón, la Comisión adopta una aproximación basada en los riesgos según la cual el marco regulatorio se aplica en principio a algoritmos de *Alto riesgo*, para lo cual es necesario establecer criterios claros de diferenciación para garantizar la seguridad jurídica. Posteriormente, este marco regulatorio podría abarcar otros algoritmos de menor riesgo o modular las obligaciones de acuerdo al riesgo, pero al menos mientras se pone en práctica debería aplicarse sólo a aquellos que representan un mayor riesgo para bienes materiales o inmateriales. En ese sentido, la aplicación de algoritmos será considerada de alto riesgo cuando cumpla con los siguientes criterios:

- Los algoritmos son empleados en sectores donde, por las características de las actividades que se realizan, se espera que los algoritmos puedan tener efectos significativos sobre las personas. Por ejemplo, el sector salud, transporte, energía, sector público, áreas de recursos humanos, etc.
- Los algoritmos son usados en el sector de tal manera que es probable que riesgos materiales o inmateriales se produzcan. La evaluación del nivel de riesgo podría basarse en el impacto en las partes afectadas. Por ejemplo, si los algoritmos producen efectos jurídicos o afectan de manera significativa los derechos de un individuo o una

empresa; o si pueden presentar riesgo de lesiones, muerte o material significativo o daño inmaterial.

- Sin perjuicio de lo anterior, se considerarán siempre de alto riesgo, con independencia del sector: los algoritmos que se apliquen para la selección de personal en empresas públicas o privadas y cualquiera que pueda afectar los derechos de los trabajadores, y los algoritmos cuyo propósito sea la identificación de características biométricas, y los algoritmos de vigilancia (Comisión Europea, 2020, pp. 17-18).

*ii. Requisitos para algoritmos de alto riesgo*

A continuación, se explicará el marco regulatorio propuesto en el Libro blanco de la Comisión Europea, el cual consta de 6 requisitos que deben cumplir las personas jurídicas, empresas, sectores, etc., de ahora en adelante, Obligados, que hagan uso de algoritmos de alto riesgo. Esta propuesta se basa en la imposición de obligaciones que permitirían la posterior auditoría por parte de las autoridades designadas por el gobierno para tal finalidad. Dicho esto, se explicará en qué consiste dicha propuesta.

Ahora bien, las consideraciones que se plantean están dirigidas a regular aspectos generales de los algoritmos. Plantear soluciones para problemáticas específicas del uso de algoritmos como las analizadas en el capítulo anterior respecto de la democracia, autonomía y opinión pública, escapa del objeto de estudio de este trabajo debido a la novedad del tema y a que proponer medidas específicas requiere de un conocimiento técnico y especializado con el cual no se cuenta sobre la tecnología misma y un estudio exhaustivo de sus efectos en estos ámbitos específicos (Comisión Europea, 2020, p. 10).

*a. Datos de entrenamiento*

Este aspecto se refiere a que los datos iniciales con los que se entrena el algoritmo garanticen que los resultados de sus análisis no conduzcan a decisiones discriminatorias. Para cumplir con este requisito, los algoritmos deben ser entrenados con bases de datos que sean suficientemente representativas, especialmente para evitar que la máquina le de un valor relevante al género, etnia y otros posibles motivos de discriminación para tomar la decisión. En segundo lugar, se debe garantizar que los datos recolectados hayan sido recolectados en

cumplimiento de las normas de protección de datos personales (Comisión Europea, 2020, pp. 18-19).

*b. Mantener registros de las bases de datos*

Teniendo en cuenta elementos como la complejidad y las dificultades relacionadas que pueden existir para verificar efectivamente el cumplimiento de las normas aplicables, se requerirá mantener un registro en relación con la programación del algoritmo, los datos utilizados para entrenarlo y, en ciertos casos, el mantenimiento de los datos mismos, así como las metodologías usadas en la programación. Estos requisitos permiten verificar acciones o decisiones potencialmente problemáticas y no solo facilitar la supervisión sino incentivar a los diseñadores de los algoritmos a cumplir con la normatividad desde una etapa temprana del diseño (Comisión Europea, 2020, p. 19).

*c. Proveer información*

Para promover el uso responsable de la inteligencia artificial es necesario proveer información de manera proactiva sobre el uso de algoritmos de alto riesgo. En ese sentido, los obligados deberán proveer información clara sobre las capacidades y limitaciones del algoritmo, en particular el propósito para el cual están destinados los sistemas, las condiciones bajo las cuales se puede esperar que funcionen según lo previsto y el nivel de precisión esperado para lograr el propósito especificado. Asimismo, deberán informar a las ciudadanos involucrados en las decisiones que esta fue tomada por un algoritmo y no por un humano (Comisión Europea, 2020, p. 20).

*d. Robustez y precisión*

La Comisión Europea considera que la robustez y precisión son requisitos necesarios para que las decisiones tomadas sean confiables. Eso significa que dichos sistemas deben desarrollarse de manera responsable y con una debida consideración previa y adecuada de los riesgos que pueden generar. En este punto, la Comisión no propone obligaciones específicas, sino que propone a los Estados implementar requisitos que garanticen que los sistemas de IA sean robustos y precisos, o al menos reflejen correctamente su nivel de precisión, durante todas las fases del ciclo de vida; requisitos para garantizar que los

resultados sean reproducibles; y, por último, requisitos que garantizan que los sistemas de IA puedan manejar adecuadamente los errores o inconsistencias (Comisión Europea, 2020, p. 20).

e. *Revisión humana*

La supervisión humana tiene como finalidad a garantizar que un algoritmo no menoscabe la autonomía humana. El objetivo de auditar algoritmos que sean confiables y éticos o solo se puede lograr asegurando una participación adecuada de los seres humanos en la toma de decisiones. La Comisión propone que la revisión humana sea necesaria para hacer efectivas las decisiones automatizadas tomadas por el algoritmo. En ese sentido, plantea que para hacer efectivo este principio, se determine que una decisión no tendrá efectos jurídicos u otro tipo de efectos a menos que haya sido revisada y validada previamente por un humano, o que esta tenga efectos desde un principio pero que se garantice la revisión humana posterior (por ejemplo, el rechazo de una solicitud de beneficios de seguridad social solo puede ser tomado por un humano) (Comisión Europea, 2020, p. 21).

f. *Otras consideraciones*

Esta propuesta no contempla la distribución de obligaciones. Es decir, el el proceso de configuración y programación de un algoritmo pueden intervenir distintos actores, tales como el diseñador y el usuario y en la medida en que se pongan en práctica estas disposiciones, se deberá determinar quién es el obligado. Desde el punto de vista de la comisión, cada obligación debe dirigirse al actor en mejor posición para abordar cualquier riesgo potencial. Asimismo, en el ejercicio de las auditorías a los algoritmos de alto riesgo, es claro que estas deben repetirse con periodicidad en tanto muchos de estos evolucionan y aprenden a partir de la experiencia, por lo cual requerirán repetidas evaluaciones en el transcurso de su uso. En cuanto a la autoridad que el Estado designe como competente, se debe asegurar que esta sea lo más independiente posible para aumentar la confianza y asegura la objetividad de las auditorías (Comisión Europea, 2020, pp. 22-26).

Si bien un país como Colombia no cuenta con el mismo desarrollo tecnológico en el campo del *big data* e inteligencia artificial que otros Estados, una regulación integral es necesaria

para que el desarrollo de esta tecnología vaya en línea con el Estado social de derecho colombiano y los ideales democráticos, para evitar abusos del poder pero también para promover la innovación en un entorno ético y respetuoso de los derechos humanos. En consecuencia, Colombia podría tomar como referencia las medidas planteadas para ser adoptadas en el ordenamiento interno teniendo en cuenta las especificaciones del entorno colombiano.

# 5. CONCLUSIONES

Después de este recorrido por las distintas aplicaciones de los algoritmos, los casos paradigmáticos y las problemáticas que se desenvuelven de estos, así como las falencias en la regulación colombiana de datos personales, podemos llegar a las siguientes conclusiones.

Por un lado, el uso de algoritmos representa grandes ventajas competitivas pero en la medida en que su aplicación se extiende a más sectores y sus funcionalidades progresan, sus utilidades se pueden volver más complejas y menos previsibles. En el segundo capítulo, se expusieron diversos casos que permiten visibilizar el uso de algoritmos a gran escala para favorecer los intereses de sectores específicos a partir del análisis masivo de datos. Tanto los algoritmos de vigilancia masiva, como de publicidad política personalizada y difusión de noticias falsas, requieren acceder a datos personales que pueden revelar los aspectos más íntimos de una personas con la finalidad de segmentar y crear perfiles y, de esta manera, operar de forma más efectiva hacia la consecución de sus objetivos.

Posteriormente, al analizar las problemáticas que derivan del uso de algoritmos para la privacidad y los datos personales, se concluye que la gran cantidad de datos disponibles sobre una persona hace que el control efectivo sobre estos por parte del titular sea difuso. La interacción de distintos servidores en plataformas de internet plantea retos importantes sobre cómo informar de manera efectiva sobre el tratamiento de datos personales y cómo ejercer vigilancia y control para asegurar que todo servidor web que procese datos personales lo haga en cumplimiento de las normas de datos personales. El segundo problema consiste en que son tantos los datos que existen sobre las personas son tan diversos que fácilmente pueden ser recolectados para realizar correlaciones en bases de datos y deducir datos personales sensibles, esto plantea un segundo reto para las normas de protección de datos en tanto estos no son entregados directamente por su titular, sino deducidos a partir de su huella digital.

En tercer lugar, características que derivan del diseño de los algoritmos como la opacidad y los sesgos implícitos, pueden fundamentar decisiones discriminatorias, desconocidas o con efectos jurídicos para el individuo. Los sesgos y la discriminación son riesgos inherentes a cualquier actividad social o económica. Sin embargo, el mismo sesgo cuando está presente en un algoritmo podría tener un efecto mucho mayor, afectando y discriminando a muchas

personas sin los mecanismos de control social que rigen el comportamiento humano (Comisión Europea, 2002, p. 11). La opacidad por su parte, que se refiere a que se desconoce la manera en que el algoritmo toma decisiones, impide que las personas perjudicadas por alguna de estas no cuenten con los elementos fácticos y técnicos suficientes para cuestionar y controvertir dichas decisiones.

En cuanto a los efectos sobre la autonomía, el riesgo pareciera radicar en que las personas cuando son objeto de decisiones automáticas o de la aplicación de un perfil, pueden desconocer los fundamentos fácticos que los llevan a optar por una decisión u otra. La afectación de la autonomía en virtud del uso de algoritmos en el ámbito de la democracia hace que cuestionemos en qué medida se transgrede el ejercicio de la deliberación que presupone que la toma de decisiones libres e informadas por parte de los ciudadanos cuando estos son sometidos a publicidad cognitiva que los incentiva a votar de una manera u otra. Por otro lado, se discute cuál puede ser el efecto de estas prácticas en la formulación de la opinión pública, la cual puede verse en potencial peligro ante la difusión de noticias falsas en públicos segmentados. Lo cierto es que aún es muy pronto para responder categóricamente a estas preguntas debido a que aún no hay estudio que teoricen sobre los efectos de los algoritmos en la organización de la sociedad y en las instituciones jurídicas actuales. En definitiva, es necesario el desarrollo doctrinal en estos temas de inminente importancia.

Se constata que el uso de algoritmos por actores estatales y no estatales en escenarios que comprometen los valores y principios democráticos manifiestan la necesidad de establecer un marco regulatorio de las tecnologías de procesamiento de la información desde la protección de datos personales y desde la regulación de los problemas que se derivan de su diseño. Se evidencia como las normas colombianas de protección de datos personales no cuentan con disposiciones específicas que permitan afrontar los nuevos retos en la materia, esto es, la creación de perfiles y decisiones automatizadas, contenidos personalizados o las deducciones de datos personales sensibles. Adicionalmente, el consentimiento informado resulta inocuo para proteger datos personales debido a que las plataformas de internet condicionan la prestación de sus servicios al otorgamiento del consentimiento, el cual puede entenderse otorgado ante conductas inequívocas, y las finalidades pueden ser aceptadas en

bloque. Como consecuencia, el consentimiento informado en Colombia no garantiza el control efectivo de los datos en cabeza de su titular.

Así, ante la ausencia de regulación en torno a los algoritmos, se expuso una posible propuesta de marco jurídico presentada por la Unión Europea, cuya pretensión es establecer ejemplos de obligaciones en cabeza de los desarrolladores de esta tecnología con la finalidad de realizar evaluaciones periódicas que acrediten la transparencia de algoritmos de alto riesgo.

Por último, es importante hacer hincapié en que cuanto más normalizada está la aplicación y el uso de algoritmos, más dificultades hay en saber cómo funcionan sus interconexiones y redes, cómo afectan nuestra organización social y los valores cívicos y éticos que estructural la sociedad (Colmenarejo, 2017, p. 86). En ese sentido, concluimos que el avance tecnológico de no es un aspecto que deba dejarse al arbitrio del libre mercado debido a los riesgos que esto conlleva. Los avances tecnológicos, en general, y los algoritmos, en específico, no deben ser ajenos a los valores fundantes de la sociedad actual ni al desarrollo sostenible. Yuval Noah Harari, en la Reunión Anual del Foro Económico Mundial de 2020, afirmó que el futuro de los algoritmos no es un problema que pueda solucionar un Estado por sí solo, se trata de un problema global, que demanda soluciones globales. Por lo cual, es necesario que la comunidad internacional fije el rumbo que debe seguir la evolución de la tecnología para asegurar la conservación del orden internacional.

# 6. BIBLIOGRAFÍA


Agencia de los Derechos Fundamentales de la Unión europea y Consejo de Europa (2014). Manual de legislación europea en materia de la protección de datos. Recuperado de: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_es.pdf

Alconada, H. (20 de septiembre de 2019). Cambridge Analytica hizo trabajos para el Pro antes de la campaña de 2015. *La Nación*. Recuperado de: https://www.lanacion.com.ar/politica/cambridge-analytica-hizo-trabajos-pro-antes-campana-nid2289827

American Civil Liberties Union (marzo 20 de 2020 de 2014). *Factsheet: The NYPD Muslim Surveillance Program.* Recuperado de: https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program

Ángel, M., & Newman, V. (2019). Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital. *DeJusticia*. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwiP_rn1nOToAhXEY98KHS2LCXIQFjABegQIBBAB&url=https%3A%2F%2Fcdn.dejusticia.org%2Fwp-content%2Fuploads%2F2019%2F01%2FRendicio%25CC%2581n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf&usg=AOvVaw0S09HcKMA6LrMK2BJXHVuh

Ardini, C., & Nahúm Mirad, H. (2020). El uso del big data en política o la política del big data. Comunicación y Hombre, (16), 225–240. Recuperado de https://comunicacionyhombre.com/wp-content/uploads/2020/01/ESTUDIO-10.pdf

Arenas, M. R. (2019). Partidos políticos, opiniones políticas e internet: la lesión del derecho a la protección de datos personales. *Teoría y realidad Constitucional*, 341-372. Recuperado de: http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=10&sid=67f1dab6-d56d-42f0-93e4-58bbd43e38bc%40sessionmgr4006

BBC (10 de junio de 2013). El hombre que reveló la amplia red de vigilancia de EE.UU. BBC. Recuperado de: https://www.bbc.com/mundo/noticias/2013/06/130610_edward_snowden_espionajes_eeuu_mr

BBC (21 de marzo de 2018). 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. *BBC*. Recuperado de: https://www.bbc.com/mundo/noticias-43472797

Bathaee, Y. (2018). The artificial intelligence, black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, (31) 2. Pp. 890-938. Recuperado de: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf

Betzu, M., Coinu, G., & Demuro, G. (2019). Gobernanza de los macrodatos y democracia representativa. UNED. *Revista de Derecho Político.* págs 253-264

Cadwalladr, C., Confessore, N., & Rosenberg, M. (Marzo 17 de 2018). How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Recuperado de: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Casas, J., Nin, J., Lópes, F. (2019). *Big Data: análisis de datos en entornos masivos*. Barcelona: Editorial UOC.

Cervantes Díaz, F. (2009). Derecho a la intimidad y habeas data. *Derecho y realidad*. p. 27-36. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiptYOEm-ToAhVpZN8KHfIbDJgQFjAAegQIARAB&url=https%3A%2F%2Frevistas.uptc.edu.co%2Findex.php%2Fderecho_realidad%2Farticle%2Fdownload%2F5010%2F4087%2F&usg=AOvVaw146kF905kbp5rRq3Jswwp0

Comisión Europea (2020). White paper on artificial intelligence - A European approach to excellence and trust. Recuperado de https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Colmenarejo, R. (2017) *Una ética para el big data: introducción a la gestión ética de datos masivos*. Barcelona, España: Editorial UOC.

Cotino, L. (2017). Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata*, 131-150. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/6066829.pdf

Corte Constitucional. Sentencia C-748 de 2011 (M.P. Jorge Ignacio Pretelt; octubre 6 de 2011).

Corte Constitucional. Sentencia T-176 de 1995 (M. P. Eduardo Cifuentes Muñoz; 24 de abril de 1995).

Corte Constitucional. Sentencia C-178 de 2014 (M. P Maria Victoria Calle; 26 de marzo de 2014).

Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, 13-36. Recuperado de: https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3351&context=bclr

de Angelis, C. (2016). La opinión pública entre la razón y el control social. Una actualización en la era del Big Data. *Avatares de La Comunicación y La Cultura*, (11). Recuperado de https://publicaciones.sociales.uba.ar/index.php/avatares/article/view/4855

Dwork, C., & Mulligan, k. (2013). It's not privacy, it's not fair. *Standford Law Review*. Recuperado el Marzo de 2020, de www.stanfordlawreview.org/: https://www.stanfordlawreview.org/online/privacy-and-big-data-its-not-privacy-and-its-not-fair/

ENISA (2015). Privacy by design in big data: An overview of privacy enhacing technologies in the era of big data analytics. Recuperado de: https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics

García (2018). Definición de servidor. [en línea] Recuperado de: https://www.economiasimple.net/glosario/servidor

Guevara, E., Medina, S., Vallejo, H. (2018). Minería de datos. *Revista científica Mundo de la investigación y el conocimiento. 2 (Especial),* pp. 339-349. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjfj-XqmuToAhVjm-AKHQkHBz8QFjAAegQIAhAB&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F6732870.pdf&usg=AOvVaw0ShJxx81EmP49Dh9XAdxz9

González, L. (2018). La crisis de la democracia representativa. nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el microtargeting y el big data. *UNED. revista de derecho político*, 257-302. Recuperado de: http://revistas.uned.es/index.php/derechopolitico/article/view/23203

González Guerrero (2018) Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros. *Estudio socio jurídico.* p. 209-245. Recuperado de: https://revistas.urosario.edu.co/index.php/sociojuridicos/article/view/6941

Greenwald, G., & MacAskill, E. (7 de junio de 2013). NSA Prism program taps in to user data of Apple, Google and others. The Guardian. Recuperado de: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Han, B. (22 de marzo de 2020). La emergencia viral y el mundo de mañana. Byung-Chul Han, el filósofo surcoreano que piensa desde Berlín. El País. Recuperado de: https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html

Harari (24 de enero de 2020). Read Yuval Harari's blistering warning to Davos in full. World Economic Forum. Recuerado de: https://www.weforum.org/agenda/2020/01/yuval-hararis-warning-davos-speech-future-predications/

Hildebrandt, M. (2008). Profiling and the rule of law. *Identity in the Information Society*, 55-70. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwij3eesp-ToAhVSTd8KHXR3AYcQFjAAegQIAhAB&url=https%3A%2F%2Flink.springer.com%2Farticle%2F10.1007%2Fs12394-008-0003-1&usg=AOvVaw2OOpMxl9wNnkGoCvS_-_fO

Holmes, D. (2017). *Big data: a very short introduction*. Oxford: Oxford University Press.

Hundt, R. (2014) Saving Privacy. *Boston Review*. Recuperado de: http://bostonreview.net/forum/reed-hundt-saving-privacy

INCLO (2018). El derecho a la privacidad en la era digital. p. 1-11. Recuperado de: https://www.cels.org.ar/web/wp-content/uploads/2018/07/INCLO-OHCHR.pdf

Kosinski, M. (2017). Big data, inteligencia artificial y el futuro de la democracia. *Aportes al Debate parlamentario*. p. 1-12. Recuperado de: http://www.bibliodigitalibd.senado.gob.mx/handle/123456789/3499

Martínez, A. (2019). la inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *La propiedad inmaterial*, 5-23. Recuperado de: http://web.a.ebscohost.com/ehost/detail/detail?vid=3&sid=e0adf27a-0ab5-46f8-bebb-bc53599915d9%40sessionmgr4008&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=137920960&db=fua

Meneses, J. (2013). Aproximación histórica y conceptos básicos de la psicometría. *UOC*. Tomado de: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/69325/4/Psicometr%C3%A

Da_Módulo%201_Aproximación%20histórica%20y%20conceptos%20básicos%20de%20la%20psicometr%C3%ADa.pdf

Metcalf, J. (16 de abril de 2018). Los efectos del escándalo de Facebook para el futuro de la democracia. MIT Technology Review. Recuperado de: https://www.technologyreview.es/s/10138/los-efectos-del-escandalo-de-facebook-para-el-futuro-de-la-democracia

Monleón-Getino, A. (2015). El impacto del Big-data en la sociedad de la información. Significado y utilidad. *Historia y comunicación social*, pp. 427-445. Recuperado de: https://revistas.ucm.es/index.php/HICS/article/view/51392

Montjoye, Y., Quoidbach, J., Robic, F. y Pentland, A. (2013). Predicting people personality using novel mobile phone-based metrics. *MIT Media Lab*. P. 1-8. Recuperado de: http://web.media.mit.edu/~yva/papers/deMontjoye2013predicting.pdf

Müller, J. (15 de febrero de 2020). La mano negra tras la crisis de Chile y Colombia. El Mundo. Recuperado de: https://www.elmundo.es/internacional/2020/02/15/5e47e31321efa09b3a8b460f.html

OCDE (2013). The OECD Privacy Framework. Recuperado de: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OCDE (22 de mayo de 2019). Cuarenta y dos países adoptan los Principios de la OCDE sobre Inteligencia Artificial. *OCDE*. Recuperado de: https://www.oecd.org/centrodemexico/medios/cuarentaydospaisesadoptanlosprincipiosdelaocdesobreinteligenciaartificial.htm

O'Neill, C. (2017). *Armas de destrucción matemática.* Madrid: Capitán Swing.

Özden, M. (2011). El derecho a la no discriminación. CETIM. Recuperado de: https://www.cetim.ch/wp-content/uploads/Derecho-a-la-no-discriminaci--n.pdf

Privacy International (2018), Las claves para mejorar la protección de datos. Recuperado de: https://privacyinternational.org/sites/default/files/2018-11/Gu%C3%ADa%20de%20Protección%20de%20Datos%20Personales_web.pdf

Remolina-Angarita, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. *International Law, Revista Colombiana de Derecho Internacional, 16. 489-524. Recuperado de:* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwivxJaxpOToAhVRhOAKHbpAAScQFjAAegQIBBAB&url=https%3A%2F%2Frevistas.javeriana.edu.co%2Findex.php%2Finternationallaw

%2Farticle%2Fview%2F13847%2F11142&usg=AOvVaw3z8qoj8C_CQHozq7VmVoAT

Riascos Gómes, L. (1997) El derecho a la intimidad, la visión iusinfirnática y el delito de los datos personales (Tesis doctoral). Universidad de Lleida, España. Recuperado de: https://www.researchgate.net/publication/297312111_El_derecho_a_la_intimidad_la_vision_iusinfirnatica_y_el_delito_de_los_datos_personales

Senso, J. y Piñero, A. (2003) El concepto de metadato. Algo más que descripción de recursos electrónicos. *Brasílica*. p. 95-106. Recuperado de: http://www.scielo.br/pdf/ci/v32n2/17038.pdf

Superintendencia de Industria y Comercio. Concepto 14-218349–00003-0000 del 24 de noviembre de 2014.

Superintendencia de Industria y Comercio. Concepto 14-218349–4- 0 del 3 de marzo de 2016.

Superintendencia de Industria y Comercio. Concepto Radicado No. 16-172268 del 9 de agosto de 2016

Talisse, R. B. (2012) Deliberation. En Estlund, D., *The Oxford Handbook of Political Philosophy* (p. 204-221). New York, New York: Oxford University Press.

Waldron, J. (2012). Democracy. En Estlund, D., *The Oxford Handbook of Political Philosophy* (p. 187-203). New York, New York: Oxford University Press.

Toscano, M. (2016). Sobre el concepto de privacidad: la relación entre privacidad en intimidad. *ISEGORÍA. Revista de Filosofía Moral y Política*. p. 533-553. Recuperado de: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiF8Jvep8roAhVsdt8KHZk8CaAQFjABegQIAhAB&url=http%3A%2F%2Fisegoria.revistas.csic.es%2Findex.php%2Fisegoria%2Farticle%2Fdownload%2F994%2F990&usg=AOvVaw0TEwXDEzL9suvwFgTkL8NS

UK Parliament (2018). Disinformation and ‘fake news’: Interim Report Contents. [en línea] Recuperado de: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36309.htm