Los derechos fundamentales en la era digital

The fundamental rights in the digital age

Viridiana Cuevas Orta[1]

Fecha de recepción: 09 de enero de 2022
Fecha de aceptación: 04 de marzo de 2022

Resumen
El desarrollo de las tecnologías de la información y comunicación ha facilitado la creación y divulgación de datos, así como la interconexión del mundo; sin embargo, ello podría representar un problema para algunos derechos fundamentales. Si bien esto puede fortalecer la capacidad de las personas para el disfrute de ciertos derechos, como la libertad de expresión, puede debilitar otros, como el derecho a la protección de datos o el derecho a la privacidad. Ello lleva a repensar sobre los profundos cambios en la sociedad y su impacto en los derechos fundamentales de las personas y llevar a debate el surgimiento de nuevos derechos fundamentales, como el derecho al olvido, el acceso universal e igualitario a nuevas tecnologías, la propiedad de los datos y su explotación y agregación al *big data,* al igual que el papel del poder público y sus modos de intervención dentro de su marco jurídico territorial.

Abstract:
The development of information and communication technologies has facilitated the creation and dissemination of data, as well as the interconnection of the world; however, this could represent a problem for some fundamental rights. While this may strengthen people's ability to enjoy certain rights, such as freedom of expression, it may weaken others, such as the right to data protection or the right to privacy. Which leads to rethink about the profound changes in society and their impact on the fundamental rights of people and lead to debate the emergence of new fundamental rights, such as the right to be forgotte, universal and equal access to new technologies, the ownership of data, and its exploitation and aggregation to big data, like the role of public power and its modes of intervention within its territorial legal framework.

1. Abogada por la Universidad de Guadalajara. Colaboradora del Instituto de Derechos Humanos Francisco Tenamaxtli de la Comisión Estatal de Derechos Humanos de Jalisco. v.cuevasorta@gmail.com

Palabras clave: Era digital, derechos fundamentales, derechos digitales.

Keywords: *Digital age, fundamental rights, digital rights.*

I. Introducción

Los avances tecnológicos dan lugar a nuevos contextos y escenarios. Se han generado cambios importantes en la manera en la que nos comunicamos e interrelacionamos. La era digital ha propiciado modificaciones en las dinámicas económicas y socioculturales. Nuestra interacción con el gobierno es, a menudo, digital, Muchas de nuestras relaciones con el sector empresarial se hacen de manera digital. En ocasiones, la forma en la que nos relacionamos con otras personas suele ser por medios digitales. Por ello, los derechos fundamentales se ven sometidos a una presión diferente a la del mundo físico. Por lo tanto, se tendría que pensar en cómo también damos forma a esos derechos fundamentales en un mundo en proceso de digitalización.

Los derechos fundamentales existentes protegen la libertad de las personas frente a los abusos cometidos por parte de autoridades. Ello es algo bueno, pero insuficiente. Es visible que las naciones no tienen poder suficiente para garantizar todas las libertades en un momento de comunicación sin fronteras, que está basado en la tecnología y el lucro. Las empresas privadas, como Google o Facebook, manejan mucha información, con efectos sobre los derechos individuales; la libertad de opinión, la protección de datos, así como la privacidad y la intimidad, por ejemplo.

La sociedad está organizada en Estados-nación con jurisdicción propia; sin embargo, el ciberespacio no conoce fronteras nacionales. Ello complica la situación y genera tensiones que solo pueden resolverse mediante una regulación internacional que armonice las legislaciones de cada país para garantizar la protección de estos derechos frente los nuevos retos tecnológicos y las libertades informativas.

II. Los derechos fundamentales

Los derechos fundamentales pueden ser entendidos como las garantías de protección que se encuentran reconocidos en los textos constitucionales y que son indispensables para el amparo de los derechos esenciales de las personas. Su protección y contenido esta circunscrito a los límites territoriales y vigencia del Estado que los reconoce (Angulo *et al.,* 2015, p. 133).

Para Ferrajoli (2001), los derechos fundamentales son todos aquellos derechos subjetivos que corresponden a todos los seres humanos, en tanto dotados del *status* de personas, ciudadanos o personas con capacidad de obrar. Se entiende

por derecho subjetivo cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica y por status; la condición de un sujeto está prevista por una norma jurídica positiva, como presupuesto de su idoneidad para ser titular de situaciones jurídicas o autor de los actos que son ejercicio de estas. (pp.19-20).

Entre las teorías que dan sustento a la noción de derechos fundamentales, se encuentra la teoría liberal, que habla de los derechos fundamentales como la libertad que toda persona tiene frente al Estado. Bajo este argumento se establece que estos derechos de libertad pueden ser entendidos como aquellas normas que especifican las competencias tanto del Estado como de los individuos (Landa, 2002, p.58). La libertad consiste en hacer todo lo que no perturbe a los otros, en consecuencia, el ejercicio de los derechos naturales de cada persona solo tiene los límites que aseguren a los otros miembros de la sociedad el disfrute de los mismos derechos. Esos límites no pueden estar determinados en la ley (Vecchio, 1968, p.39).

La teoría axiológica de los derechos fundamentales se basa en la concepción del Estado como una comunidad política en permanente proceso de integración en torno a valores, creencias y cultura. Los derechos y libertades se reconocen como instrumentos, cuyo ejercicio se propicia y fomenta ese proceso de integración. El ámbito y contenido de los derechos se define con arreglo a esa función de preservación y fomento de tales valores (Bastida et al., 2004, p.62). Someter los derechos fundamentales a la valoración intuitiva o al estado de conciencia social, en etapas de rápidas transformaciones y cambios, permite suponer la modificación o la afectación de los valores supremos y eternos de una sociedad, donde el carácter preexistente y vinculante de los principios y valores que dan sentido a la unidad de una comunidad no permanezca estable o inmodificable. En este sentido, los derechos fundamentales se relativizan a su tiempo y espacio, revaluándose o devaluándose, según las circunstancias del estado de conciencia o del espíritu del momento Zeitgeist[2] (Böckenförde,1993, p.59).

La expresión derechos fundamentales engloba varios preceptos de suma importancia dentro del ordenamiento jurídico contemporáneo. Ello conduce al análisis de los principios, especialmente el de dignidad humana, como fundamento básico del Estado democrático de derecho (Do Amaral, 2014, p.22). Acorde con el sistema de valores de Günter Dürig (en López, 2016, p.152), la dignidad humana es el valor supremo del ordenamiento jurídico. Así, de la dignidad humana se desprenden todos los derechos fundamentales entendidos como valores, principalmente, la libertad y la igualdad, y de ellos todos los demás, por lo que la dignidad funciona como criterio interpretativo de todos los derechos, donde cualquier violación de estos es una violación de la dignidad humana y cualquier violación de esta es una violación de los derechos fundamentales (Anzures, 2017, p.60)

2. Es una palabra en alemán que puede traducirse al español como «espíritu del tiempo» o «espíritu de la época». Hace referencia al clima, ambiente o atmósfera intelectual y cultural de una determinada era.

III. La revolución digital y los derechos humanos

PAl igual que las revoluciones industriales anteriores, la transformación digital sacude todos los modelos económicos, tecnológicos y sociales habituales. Los efectos de la revolución de la información son más visibles ahora. Todo se pone a prueba, desde el modelo de negocio hasta la comunicación privada y, por consiguiente, las reglas sociales también se ven afectadas. Ello guarda un gran parecido con las reacciones al final de la revolución industrial. Al principio, no había leyes sociales, se tuvo que esperar hasta que los efectos negativos del capitalismo fueran visibles.

La difusión y desarrollo de este sistema tecnológico ha cambiado la base material de nuestras vidas, por lo tanto, de la vida misma en todos sus aspectos: en cómo producimos, cómo y en qué trabajamos, cómo vendemos, cómo y qué consumimos, cómo nos educamos, cómo nos informamos, cómo nos entretenemos, cómo gobernamos, cómo hacemos la guerra y la paz, cómo nacemos y cómo morimos, y quién manda, quién se enriquece, quién explota, quién sufre y quién se margina. Acorde con Castells (2016), el desarrollo de las tecnologías de información no determina lo que sucede en la sociedad, pero pueden cambiar profundamente las reglas del juego, que debemos aprender de nuevo y de manera colectiva y saber cuál es nuestra nueva realidad o sufriremos, individualmente, el control de los pocos (países o personas) que conozcan los códigos de acceso a las fuentes de saber y poder (párr.1).

Con el internet, es plausible hacer cosas que no eran posibles hace cincuenta años. Sin embargo, cualquier forma de libertad puede dar lugar a abusos; el ciberdelito,[3] por ejemplo. En este caso, debemos hacer una pausa y comprobar que las leyes existentes y que sus instrumentos sean suficientes. El apoyo a la innovación implica pasar de una lógica reglamentaria a una regulatoria, es decir, a un tipo de supervisión y apoyo que combine la fidelidad a los principios fundamentales y a un claro Estado de derecho, así como nuevos modos de intervención reguladores a nivel internacional.

III.1 Algoritmos[4] y derechos fundamentales

Los mundos físico y digital están inextricablemente vinculados y muchas decisiones importantes ya no las toman los humanos, sino las computadoras. La aparición de tecnologías impulsadas por algoritmos, como big data, el internet de las cosas (IoT)[5] y la inteligencia artificial (IA), son importantes impulsores de este proceso de digitalización. Estas tres tecnologías pueden hacer que funcionen los gobiernos, las empresas y la vida cotidiana de muchas personas y, además, muestran un alto grado de coherencia.

IoT se refiere al desarrollo en el que cada vez más dispositivos "cotidianos" están conectados a internet. Dichos instrumentos pueden percibir, transmitir

3. El ciberdelito o delito informático es todo aquel acto ilegal realizado por un ciberdelincuente en el espacio digital a través de las redes informáticas y diversos dispositivos electrónicos. Dichos actos ilegales atentan a la integridad y confidencialidad de los datos y de los sistemas informáticos y tienen el objetivo de estafar y robar datos.
4. La Real Academia define algoritmo como un "conjunto ordenado y finito de operaciones que permite hallar la solución de un problema". Un algoritmo de búsqueda en internet es un conjunto de instrucciones que describen el procedimiento a seguir para alcanzar un resultado determinado y específico en la web. Esto dentro de una estructura de datos de gran relevancia.
5. Por sus siglas en inglés, Internet of Things.

y transportar datos y contribuir a una digitalización del mundo físico de gran alcance.

Esta digitalización tiene un enorme aumento de datos. Los gobiernos y las empresas son cada vez más capaces de extraer información relevante a partir de grandes cantidades de datos variados, en su mayoría, en tiempo real, y utilizarlos para la toma de decisiones (automatizada). Esta se conoce como el proceso de big data.

La IA se centra en computadoras que pueden imitar la inteligencia humana. Esta puede proporcionar la tecnología para los identificadores con los que se pueden realizar análisis de datos complejos. Esto significa que la IA puede ser importante para los procesos de big data y para procesar los datos recopilados por los dispositivos conectados a internet. Las tres tecnologías también tienen en común que los algoritmos forman un componente tecnológico crucial en su funcionamiento.

La unión de los tres desarrollos tecnológicos impulsados por algoritmos puede tener un impacto importante en la vida de las personas y, por lo tanto, en el ejercicio de los derechos fundamentales. Ello debido a la enorme cantidad de aplicaciones inmersas en estas. Desde la atención médica y la investigación de delitos hasta el sector financiero y el entorno de vida espacial; ningún dominio es inmune a los cambios que se producen bajo la influencia del big data, el IoT y la IA, especialmente la influencia de los algoritmos que unen estas tecnologías.

III.2 Big data

Los datos son bloques de construcción indispensables para la adquisición de conocimientos (Kitchin, 2014, p. 1). Por lo tanto, el procesamiento de datos es algo que se ha realizado durante años. Los censos manuales de registro de población son ejemplos tempranos de la adquisición de conocimientos e información mediante el compendio de datos a gran escala. La recopilación y el procesamiento de datos originalmente era un asunto costoso y que requería mucho tiempo. Una ola de desarrollos en el campo de las tecnologías de la información y la comunicación ha llevado al aumento significativo de las posibilidades de compilación y manejo de datos. Ahora vivimos en una "era de datos" (White, 2015, p.3).

Este proceso ha llevado a que nuestras vidas se desarrollen cada vez más en línea (Kitchin, 2014, p. 80-81). Además, en este mundo digital, los datos se pueden recopilar y almacenar fácilmente. Las tecnologías para conectar datos han propiciado su conversión en información relevante. Por lo tanto, el aumento de datos conduce a un mayor conocimiento. Bajo la influencia de desarrollos anteriores, los datos se han convertido en "big" y "big data" se ha convertido en un término de uso común.

Los retos que surgen de esta herramienta de análisis incluyen las responsabilidades tanto de las empresas privadas como lo ha puesto de manifiesto la Organización de Naciones Unidas (ONU) a través de los Principios rectores sobre las empresas y los derechos humanos (2011). Puestos en práctica en el marco de las Naciones Unidas para "proteger, respetar y remediar", donde se especifica que es responsabilidad de las empresas "abstenerse de infringir los derechos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación" (p. 15). Las compañías que realizan este análisis tienen la obligación y la responsabilidad de respetar "los derechos humanos internacionalmente reconocidos que abarcan, como mínimo, los derechos enunciados en la Carta Internacional de Derechos Humanos" (2011, p. 15). Además, si se determina que las empresas "han provocado o contribuido a provocar consecuencias negativas, deben repararlas o contribuir a su reparación por medios legítimos" (2011, p.28). Como ejemplo existe la Armada Electrónica Siria (SEA),[6] que, en 2011, utilizó cuentas de Facebook falsas, software de monitoreo y virus informáticos (como troyanos y malware) para conocer las prácticas de los disidentes del gobierno (Nersessian, 2018, p. 848).

Autores como Ureña (2019, p.100) y Sarfaty (2018, p.76) opinan que las técnicas de análisis de big data se pueden utilizar para prevenir posibles violaciones de derechos humanos. Gracias a la posibilidad de obtener grandes volúmenes de datos, es factible hacer mediciones, predicciones y, con base en ello, realizar la toma de decisiones sobre distintos asuntos de una manera más informada. Ambos autores consideran que el big data puede ser una herramienta de gran utilidad para los derechos humanos; sin embargo, también dejan ver los posibles riesgos que pueden generarse por una mala programación o utilización de la información que se genera mediante estos análisis de datos.

III.3 Internet de las cosas

Conectar "cosas" a internet es anterior al uso del término internet de las cosas (IoT). Este último consiste en la idea de conectar varios dispositivos u objetos (cosas) mediante conexiones inalámbricas, por cable y esquemas de direccionamiento únicos y crear un entorno generalizado, donde una persona pueda interactuar en cualquier momento con el mundo digital y el físico. También abarca objetos y máquinas virtuales, que tienen atributos digitales y personalidades en evolución (Baldini et al., 2015, p.10). El desarrollo del IoT es el resultado de la convergencia y el rápido avance de tecnologías ya existentes (Poudel, 2016, p. 999). Los hogares y ciudades inteligentes y las aplicaciones para la salud, son algunos ejemplos de ello.

En un hogar inteligente, los instrumentos e instalaciones electrónicas, como los electrodomésticos, la instalación eléctrica, televisores, dispositivos de sonido, sistemas de seguridad y cámaras, están conectados entre sí y a internet, ello se conoce como *domótica.*[7] Son capaces de comunicar e intercambiar información

6. Por sus siglas en inglés, Syrian Electronic Army, es un grupo de hackers informáticos que apareció por primera vez en línea en 2011 para apoyar al gobierno del presidente sirio Bashar al-Assad. Utilizando spam, desfiguración de sitios web, malware, phishing y ataques de denegación de servicio, se ha dirigido a organizaciones terroristas, grupos de oposición política, medios de comunicación occidentales, grupos de derechos humanos y sitios web que aparentemente son neutrales al conflicto sirio.
7. Se llama así a los sistemas capaces de automatizar una vivienda o edificación de cualquier tipo, que aportan servicios de gestión energética, seguridad, bienestar y comunicación, y que pueden estar integrados mediante redes interiores y exteriores de comunicación, cableadas o inalámbricas, cuyo control goza de cierta ubicuidad desde dentro y fuera del hogar. Se podría definir como la integración de la tecnología en el diseño inteligente de un recinto cerrado.

y pueden responder entre sí y con los residentes. La característica de un hogar inteligente es que se anticipa al usuario, se adapta proactivamente y ofrece servicios a la medida, en ocasiones antes de que la o el residente sea consciente de sus necesidades. Dichas herramientas generan datos que son analizados por algoritmos, ello lleva a una voluntad propia del hogar.

Una ciudad inteligente utiliza los datos recopilados en tiempo real por objetos equipados con sensores que están conectados a internet. Esta información es utilizada para monitorear y regular los flujos de tráfico y los patrones de emisión asociados a estos; en los sistemas de navegación de los automovilistas, se usa para recibir información sobre la ruta a recorrer; el alumbrado público puede adaptarse a la hora del día, las condiciones climáticas y la proximidad y el estado de ánimo de las personas. Los datos se pueden combinar y utilizar para monitorear el bienestar y seguridad en la ciudad inteligente. El conocimiento adquirido puede conducir automáticamente a ajustes en el entorno físico de vida de la ciudadanía.

Las aplicaciones para la salud son aquellas cuya tecnología tiene como propósito principal mejorar la salud y el bienestar. Los dispositivos utilizados en la salud humana se dividen en tres categorías: aquellos diseñados para ser usados o transportados (*wearables*),[8] los instrumentos inteligentes que se insertan, inyectan o tragan, y las herramientas de medición no portátiles, que son las que recopilan y transmiten datos de salud del cuerpo humano periódicamente, pero no están conectadas continuamente, como los oxímetros de pulso habilitados para bluetooth o las básculas habilitadas para Wi-Fi (McKinsey Global Institute, 2015, p.38).

El IoT abre nuevas e interesantes oportunidades, pero también nuevas preguntas sobre la interacción entre la ciudadanía, los gobiernos y las empresas que operan en el mundo digital. Algunas de estas cuestiones incluyen la captura, procesamiento y la propiedad de los datos de las y los ciudadanos y la posible necesidad de crear nuevos marcos legislativos o técnicos para ejercer más control sobre un entorno tan grande y complejo y, simultáneamente, evitar imponer restricciones innecesarias al desarrollo del mercado de IoT (Baldini et al., 2015, p.10).

III.4 Inteligencia artificial

Para Nilsson (2010), la inteligencia artificial (IA) es aquella actividad dedicada a hacer que las máquinas sean inteligentes, e inteligencia es aquella cualidad que permite que una entidad funcione apropiadamente y con previsión en su entorno (p.13). La IA se caracteriza por un alto grado de autonomía. Las aplicaciones de IA pueden realizar tareas complejas sin guía ni control humanos. El problema de control relacionado con la IA es que existe la posibilidad de que los sistemas de IA tengan tal grado de autonomía que ya no sea posible que sea controlada por los humanos.

8. La palabra wearable posee una raíz inglesa, cuya traducción significa "llevable" o "vestible".

La IA tiene una multitud de subáreas, incluido el procesamiento del lenguaje natural,[9] sistemas expertos (aquellos que tienen conocimiento de un área determinada); por ejemplo, en un entorno médico y la robótica.[10] La combinación de desarrollos en estas subáreas ha dado como resultado que la IA cubra un amplio espectro de aplicaciones. Muchas de las aplicaciones de big data e IoT tienen interfaces[11] con IA.

Los riesgos creados por la autonomía de la IA abarcan no solo cuestiones de previsibilidad, sino también problemas de control. Puede resultar difícil para los humanos mantener el control de las máquinas que están programadas para actuar con una autonomía considerable. Existe una gran cantidad de mecanismos por los que se puede producir una pérdida de control: un mal funcionamiento, como un archivo corrupto o daño físico al equipo de entrada; una brecha de seguridad; el tiempo de respuesta superior de las computadoras en comparación con los humanos (Johnson et al, 2013; en Scherer, 2016, p.366) o una programación defectuosa. El control, una vez perdido, puede ser difícil de recuperar, si la IA está diseñada con características que le permiten aprender y adaptarse.

Varias características de la IA harán que sea excepcionalmente difícil regularla en comparación con otras fuentes de riesgo público. El creciente papel de la IA en la economía y la sociedad presenta desafíos tanto prácticos como conceptuales para el derecho. Muchos surgen de la forma en que se investiga y desarrolla la IA y del problema básico de controlar las acciones de máquinas autónomas (Vladeck, 2014; en Scherer, 2016, p.121.) Los retos conceptuales nacen de las dificultades para atribuir la responsabilidad moral y jurídica de daños causados por máquinas autónomas y del rompecabezas de definir qué significa exactamente inteligencia artificial, por lo que puede resultar complicado garantizar que las partes perjudicadas reciban una compensación cuando un sistema de IA cause daños.

IV. El reconocimiento de nuevos derechos fundamentales y su protección

ELos avances tecnológicos están cambiando la forma en la que se ejercen, se vulneran y se protegen derechos fundamentales, como la libertad de expresión o el acceso a la información, a la vez que se da el reconocimiento de nuevos derechos, ello conlleva la necesidad de un nuevo marco de regulación. Las leyes se están teniendo que adaptar a esta era digital, como consecuencia de ello, ha surgido el desarrollo de los derechos digitales.[12]

Existe un consenso creciente de que el uso, procesamiento e intercambio de datos en diferentes tecnologías debe cumplir con los principios básicos de los derechos humanos. La esencia clave de un enfoque centrado en los derechos humanos es proteger la dignidad y los derechos de las personas, ello requiere que los gobiernos respeten, protejan y cumplan los derechos humanos. Esto implica varias responsabilidades, como proteger a las personas y reparar los daños derivados de las tecnologías basadas en datos. Un enfoque centrado en los

9. La capacidad de procesar y producir lenguaje hablado y escrito.
10. Máquinas que pueden realizar tareas programables.
11. Se utiliza en informática para nombrar a la conexión funcional entre dos sistemas, programas, dispositivos o componentes de cualquier tipo, que proporciona una comunicación de distintos niveles y permite el intercambio de información.
12. Los derechos digitales son aquellos que permiten a las personas acceder, usar, crear y publicar medios digitales, así como acceder y utilizar ordenadores, otros dispositivos electrónicos y redes de comunicaciones.

derechos humanos también conlleva proteger la privacidad de las personas.

El derecho a la protección de los datos personales y el derecho al acceso a internet nació como respuesta a las preguntas planteadas por el boom digital. Suelen estar relacionados respectivamente con el derecho a la privacidad y la libertad de expresión; sin embargo, sus intereses son más amplios y pueden considerarse como derechos fundamentales autónomos.

Los derechos digitales representan una adaptación de la Declaración Universal de los Derechos Humanos[13] (1948) de la Organización de las Naciones Unidas (ONU) aplicada al mundo en línea, cuyo principal objetivo es garantizar el acceso a internet y que ello reduzca la brecha digital.

IV.1 El acceso a la información

El internet es una red de redes interconectadas entre sí, la persona que cuente con acceso a este servicio tiene, además de la posibilidad de interactuar con otros usuarios, la disponibilidad de un sinfín de datos, documentos y contenidos de diversos temas que han sido aportados por otros usuarios. Sin embargo, el acceso a la cantidad de información puede verse limitado por las condiciones geográficas, materiales y culturales en las que se encuentre la persona.

El derecho de acceso a la información se basa en el derecho más amplio a la libertad de expresión y abarca el derecho de toda persona a buscar y obtener información en poder de las autoridades públicas. El derecho a la libertad de información fue reconocido por primera vez en la Ley de Libertad de Prensa en 1776.

El artículo 19 de la Declaración Universal de los Derechos Humanos (1948) establece que:

> Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión (p.6).

De lo anterior se desprende que el derecho a la información es una facultad esencial de cada persona de atraerse información, es decir, para ser informada y poder informar. Sin embargo, esas libertades no han de ser ilimitadas y deben ser compatibles con los derechos humanos de terceros, pues estos requieren tener, como fin último, proteger y hacer efectiva la dignidad humana (Muhlia, 2008, p.3).

El Pacto Internacional de Derechos Civiles y Políticos (1966), en su artículo 19, señala que:

13. Este instrumento internacional fue adoptado por la Organización de las Naciones Unidas el 10 de diciembre de 1948. Respecto a este instrumento internacional, existe discrepancia de criterios en torno a su carácter vinculatorio, en virtud de su naturaleza declarativa; sin embargo, en la práctica, no resulta factible negarle validez jurídica, pues forma parte de los estándares universalmente compartidos en la materia.

> Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística o por cualquier otro procedimiento de su elección (p.7).

Por su parte, la Convención Americana sobre Derechos Humanos[14] (1969), en su artículo 13 establece que "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole" (p. 7); además, señala que:

> No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

En México, la Constitución Política de los Estados Unidos Mexicanos (1917), en su artículo 6°, menciona que:

> ...El derecho a la información será garantizado por el Estado…Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión…. El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.

La finalidad del Estado es velar por el bien común de la ciudadanía, por su pleno e integral desarrollo, mientras que el derecho de acceso a la información, entendiéndolo como un derecho humano, hace exigibles las garantías individuales que reconoce la constitución (Muhilia, 2008, p.56); es un mecanismo para acceder a la igualdad no solo entendida como el derecho a la no discriminación, sino como el derecho al goce de ciertos derechos fundamentales.

IV.2 El derecho a la privacidad

El derecho a la privacidad o la intimidad es aquel derecho humano por virtud del cual la persona, llámese física o moral, tiene la facultad o el poder de excluir o negar a las demás personas el conocimiento de su vida personal, además de determinar en qué medida o grado esas dimensiones de la vida personal pueden ser legítimamente comunicados a otros (Martínez, 2000; en Estrada, s.f., p.3). La privacidad es un elemento importante en la autonomía de la persona. Mucho de lo que nos hace humanos proviene de las interacciones con otras personas dentro de una esfera privada, donde se asume que nadie nos observa. La privacidad se relaciona con lo que decimos, lo que hacemos y quizá con lo que sentimos (MacMenemy, 2016, pp.1-2).

El derecho a la privacidad en la era digital se ve altamente vulnerado por la automatización de datos. En la resolución 73/179 de 2018, emitida por la

14. Este instrumento internacional fue adoptado en la ciudad de San José, Costa Rica, el 22 de noviembre de 1969; fue aprobado por el Senado de la República el 18 de diciembre de 1980, lo cual consta en el Diario Oficial de la Federación del 9 de enero de 1981. Dicho instrumento entró en vigor en el ámbito internacional el 18 de julio de 1978, pero, para el Estado mexicano, no fue sino hasta el 24 de marzo de 1981, previa su adhesión en esa misma fecha y su promulgación en el Diario Oficial de la Federación el 7 de mayo de 1981.

Asamblea General de las Naciones Unidas (2018), sobre el derecho a la privacidad en la era digital, se señala que:

> …el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los Gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, establecido en el artículo 12 de la Declaración Universal de Derechos Humanos (1948) y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1976), y que, por lo tanto, esta cuestión suscita cada vez más preocupación (Asamblea General de las Naciones Unidas, 2018, p.2).

Además, se resalta la preocupación de "que las violaciones y las transgresiones del derecho a la privacidad en la era digital pueden afectar a todos los individuos y tener repercusiones particulares en las mujeres, así como los niños y las personas vulnerables y marginadas" (Asamblea General de las Naciones Unidas, 2018, p.2).

Por otra parte, es importante analizar que la privacidad es una característica indispensable de una democracia, donde una persona mantiene su identidad mientras contribuye a su deber cívico. Spiros Simitis (1985) reconoció los riesgos que la automatización de datos causaría a la privacidad, a las personas y a los procesos democráticos. También identificó que la privacidad no es un fin en sí mismo, sino un medio para lograr un cierto ideal de política democrática, en el que se confía en que las y los ciudadanos sean más que meros proveedores de información satisfechos de sí mismos para tecnócratas que todo lo ven y todo lo optimizan (párr.16).

Tres tendencias tecnológicas sustentaron el análisis de Simitis. En primer lugar, señaló que todas las esferas de interacción social estaban mediadas por la tecnología de la información: advirtió sobre la recuperación intensiva de datos personales de prácticamente todos los empleados, contribuyentes, pacientes, clientes bancarios, beneficiarios de asistencia social o conductores de automóviles. Como resultado, la privacidad ya no era solo un problema en el que alguna persona era atrapada con la guardia baja en una situación incómoda, sino que se había convertido en un problema donde todas las personas se encontrarían expuestas. En segundo lugar, las nuevas tecnologías, como las tarjetas inteligentes y el videotexto,[15] no solo hacían posible registrar y reconstruir actividades individuales con todo detalle, sino que también normalizaban la vigilancia, entretejiéndola en la vida cotidiana. En tercer lugar, la información personal registrada por estas tecnologías permitía a las instituciones sociales imponer estándares de comportamiento, ello desencadena estrategias de manipulación a largo plazo destinadas a moldear y ajustar la conducta individual (párr.18).

15. Sistema que permite a un usuario acceder desde un ordenador personal a datos procedentes de grandes bases de datos mediante conexión telefónica permite acceder a una cantidad de información prácticamente ilimitada.

IV.3 Protección de datos personales

El primer instrumento internacional jurídicamente vinculante para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal fue el Convenio n° 108 del Consejo de Europa (1981), cuya finalidad es garantizar a cualquier persona física el respeto de sus derechos y libertades fundamentales, específicamente, su derecho a la vida privada, según el tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (Maciejewski, 2021).

A lo largo del tiempo, diversos países han legislado en materia de protección de datos. Tal es el caso de la Datenschutz alemana, de 1970; la Privacy Act de los Estado Unidos, de 1974; la Ley Orgánica de España de 1999 sobre la Protección de Datos de Carácter Personal; la Ley 29.733 peruana, de 2011, y la Ley Federal de Protección de Datos Personales en Posesión de Particulares mexicana (Sánchez y Rojas, 2012, p.6).

Asimismo, la Carta de Derechos Fundamentales de la Unión Europea (2000) contempla, en su artículo 8, la protección de datos de carácter personal, al considerar que:

> […] 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 su rectificación.

En el mundo, existen dos vertientes principales en torno a la protección de los datos personales: el modelo europeo busca proteger la información y la propiedad de esta, en aras de conservar la honorabilidad de la persona, aun cuando esta hubiese fallecido, la motivación de este modelo tiene base en los derechos humanos de los individuos. El modelo estadounidense pretende proteger la información de las personas con el concepto de derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto, este tipo surge derivado de motivos comerciales, pues las empresas utilizaban de manera indiscriminada esa información (Sánchez y Rojas, 2012, p.4).

En 2018, se reveló que algunas corporaciones tecnológicas habían hecho un uso ilegal de datos personales de usuarios de redes sociales para hacer campañas políticas, tal es el caso de Cambridge Analytica,[16] empresa que utilizó los datos de millones de usuarios de Facebook Inc. mediante una aplicación en la que se realizaban cuestionarios sobre personalidad desarrollados por dos psicólogos del Pyschometrics Centre en la Universidad de Cambridge, donde los usuarios que aceptaban realizar los cuestionarios daban su consentimiento para que la aplicación recabara, de forma anónima, información almacenada tanto en sus perfiles personales como en el de sus contactos, con ello se obtuvo información de 50 000 000 millones de usuarios (Wylie, s.f., en The Guardian,2018, párr.16), que serviría para influir en la opinión de la gente a través de campañas publicitarias

16. Era una empresa británica dedicada a las consultorías de mercado y las campañas electorales.

que ayudarían a Trump a ganar las elecciones en 2016.

El análisis de estos hechos muestra el estado actual del derecho humano a la privacidad que tienen las poblaciones: la privacidad vale cada vez menos, se ve vulnerada mediante modelos de negocios de las corporaciones que venden publicidad/propaganda. Este es un campo minado de interpretaciones tendenciosas, corporativas y para-legales, pues las regulaciones actuales, lejos de servir a los usuarios y la ciudadanía, parecen solo estar el servicio del mercado ilegal-negro de datos personales. Estos sucesos muestran la fragilidad y desprotección de este derecho (Verselli, s.f., pp.8-9).

VI.4 Derecho al olvido

SiEl derecho al olvido se refiere a la capacidad de las personas para borrar, limitar, desvincular, eliminar o corregir información personal en internet que sea engañosa, vergonzosa, irrelevante o anacrónica (Kelly y Satola, 2017). El concepto de derecho al olvido en internet fue reconocido por primera vez con la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) del 13 de mayo de 2014 en el caso Google Inc. vs. la Agencia Española de Protección de Datos (AEPD).

El 5 de marzo del 2010, un ciudadano español presentó una reclamación ante la AEPD contra Google Spain y Google Inc., donde argumentó que, cuando se introducía su nombre en el motor de búsqueda[17] de Google, aparecían un par de páginas web de un periódico en las que se anunciaba una subasta de inmuebles relacionada a un embargo por deudas a la Seguridad Social; sin embargo, dicho asunto había sido resuelto varios años atrás, por lo que exigía al periódico eliminar o modificar la publicación para que no aparecieran sus datos personales y, por otro lado, solicitaba que se le exigiera a Google Spain o Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de aparecer en los resultados de búsqueda.

La AEPD determinó que la publicación en la página era legítima y que el buscador Google debía remover los enlaces de sus resultados de búsqueda e imposibilitar el acceso a estos en el futuro. Tanto Google Spain como Google Inc. presentaron recursos para solicitar que se anulara la resolución (Guerrero, 2018, p. 57).

Al analizar estas cuestiones, el tribunal llega a la conclusión, en términos generales, de que efectivamente la normativa europea (tanto de la Unión Europea como la española que la extrapola) resulta aplicable a Google Spain; pues los proveedores de servicios de motor de búsqueda se consideran responsables del tratamiento de datos personales y, en consecuencia, reconoce la posibilidad de que el interesado (titular de los datos) solicite que sus datos personales como criterios de búsqueda y, específicamente su nombre, dejen de estar vinculados a determinadas páginas web fuente. Cabe añadir el énfasis del tribunal para

17. Un motor de búsqueda web es un programa que "trae a la superficie" los resultados de muchos sitios web que considera los más adecuados para satisfacer la necesidad o razón por la que alguien escribió su consulta de búsqueda.

considerar que la información estructurada que arroja un motor de búsqueda sobre una persona física genera una afectación significativa de la vida privada y de la protección de datos personales (Maqueo, 2015, párr.7).

Dicha resolución del TJUE sienta un importante precedente para abordar las pretensiones de los particulares en el ejercicio de su derecho a la autodeterminación informativa (Basterra, 2008, p.26)

En México, se inició, en 2014, un procedimiento ante el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), donde la persona titular de los datos personales solicitaba que se le ordenara a Google México remover de sus resultados de búsqueda una nota publicada en una revista en línea donde se le vinculaba con un posible fraude y tráfico de influencias, información que consideró que afectaba su honor y su vida privada, así como sus relaciones comerciales y financieras actuales (Guerrero, 2018, p.58).

El IFAI le dio la razón, reconociendo el derecho al olvido, es decir, consideró que un particular puede pedir a Google México que omita arrojar en los resultados de su búsqueda notas o entradas relacionadas con su nombre, pues al presentar esos resultados en pantalla adquiere la calidad de responsable del tratamiento de datos personales y con ello se obliga a respetar los derechos de acceso, rectificación, cancelación y oposición (ARCO) de datos personales, derechos fundamentales hoy reconocidos en la Constitución Política de los Estados Unidos Mexicanos (1917), en su artículo 16, párrafo segundo (López, 2015, párr.1).

Toda decisión de autoridad que ordene a un buscador de internet (como Google) dejar de mostrar ciertos resultados tiene que ser objeto de un ejercicio de ponderación, a fin de tratar de encontrar un equilibrio entre el derecho de quien se dice afectado, el interés público de que la información pueda seguirse exhibiendo en los resultados de la búsqueda y la libertad de expresión. Este principio se encuentra contenido en los artículos 26 y 34 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (López, 2015, párr.5).

V. Conclusiones

El desarrollo de nuevas tecnologías de la información y la comunicación presenta una amplia gama de nuevos desafíos constitucionales. La digitalización tiene un impacto en el Estado de derecho y democracia.

El mundo digital se basa completamente en datos y, en particular, aquellos que son personales. Gracias a dicha información, es posible establecer una conexión entre los diferentes ámbitos de la vida pública y privada de una persona, pues se obtienen datos relacionales, de ocio, ideológicos, de salud e incluso de geolocalización.

Dicha capacidad de recopilar datos extremadamente particulares y, si es necesario, hacer referencias cruzadas, es lo que está en el centro del surgimiento de nuevos servicios. Por lo tanto, la tecnología digital permite una red de información sin precedentes, atractiva tanto para los actores privados como para las autoridades públicas. Sin embargo, dicha captación de datos es por lo regular generada de forma voluntaria, es decir, se suelen llenar formularios de cláusulas o términos cada vez que una persona se da de alta en alguna red social o se registra en algún sitio web. Se aceptan casi de manera automática las condiciones y no se suele ser consciente de lo que se admite porque no se da el tiempo de leer; esa captación de datos y lo que se puede hacer con ellos puede vulnerar ciertos derechos.

Los derechos fundamentales, como la libertad de expresión, la igualdad de trato, la privacidad, la intimidad y el acceso a la justicia, resultan relevantes en la era digital, donde los datos personales se recopilan y procesan a gran escala para tomar decisiones sobre las personas. La protección de los derechos fundamentales debe ser exigible frente a los Estados y las empresas (Spitz, 2015, párr.7).

Por otro lado, el alcance y funcionamiento, incluido el nivel de protección, que ofrecen la mayoría de los derechos fundamentales actuales puede ser diferente en un contexto digital. Por ejemplo, el derecho a un juicio justo y el acceso a los tribunales, que son fundamentales en las sociedades democráticas, pueden verse desde una perspectiva completamente nueva a la luz de los desarrollos en la IA que se adapta a la judicatura. Si la IA llega a predecir con precisión los resultados de los tribunales, esta podría hacerse cargo de las decisiones judiciales a largo plazo.

VI. Referencias Bibliográficas

Angulo, G., López, J. (2015). *Teoría contemporánea de los derechos humanos: elementos para una reconstrucción sistemática.* Madrid. Dykinson. p.133.

Anzures, J. (2010). *La eficacia horizontal de los derechos fundamentales. Cuestiones constitucionales.* (22), pp.3-51. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405919320100001000001&lng=es&tlng=es

Anzures-Gurría, J. (2017). *La dimensión objetiva de los derechos fundamentales en México.* Díkaion, 26(1), pp.53-83. https://doi.org/10.5294/dika.2017.26.1.4

Asamblea General de las Naciones Unidas. (2018). *Resolución 73/179 de "El derecho a la privacidad en la era digital"* A/RES/73/179 https://undocs.org/pdf?symbol=es/A/RES/73/179

Asamblea General de las Naciones Unidas. (2019). *Resolución aprobada por la Asamblea General el 17 de diciembre de 2018.* https://undocs.org/pdf?symbol=es/A/RES/73/179

Baldini, G., Peirce, T., Botterman, M., Talacchini, M., Pereira, A., Handte, M., Rotondi,

D., Pöhls, H., Vermesan, O., Baddii, A., Copigneaux, B., Schreckling, D., Vigano, L., Steri, G., Piccione, S., Valcheas, P., Stavroulaki, V., Kelaidonis, D., Neisse, R.,… Skarmeta, A., (2015). Internet of Things. *IoT Governance, Privacy and Security Issues.* http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf.

Basterra, M. (2008). *Protección de datos personales.* Ley 25.326 y Dto. 1558/01 Comentados. Derecho constitucional provincial Iberoamérica y México. Buenos Aires. Ediar-UNAM. p.26.

Bastida, F., Villaverde, I., Requejo, P., Presno, M., Alaéz, B., Sarasola, I. (2004). *Teoría general de los derechos fundamentales en la Constitución Española de 1978.* Madrid. Tecnos. p.62.

Böckenförde, E. (1993). *Escritos sobre Derechos Fundamentales.* Alemania. Nomos Verlagsgesellschaft, p.59.

Carrouche, Daian (2016). *Los ciber derechos: los derechos humanos en la era digital.* Documento inédito, Universidad Católica Argentina, Facultad "Teresa de Ávila", Departamento de Derecho, pp.7-11. http://bibliotecadigital.uca.edu.ar/repositorio/contribuciones/ciber-derechos-era-digital.pdf

Castells, M. (2016). Tribuna: La sociedad de la información en http://elpais.com/diario/1995/02/25/opinion/793666808_850215.html

Conde, C. (2005). *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad.* Madrid. Dykinson, p. 27.

Constitución Política de los Estados Unidos Mexicanos (1917). *Diario Oficial de la Federación.* Octubre 10 2021. México. http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf

Convención Americana sobre Derechos Humanos. (1869). Costa Rica. https://www.corteidh.or.cr/tablas/17229a.pdf

Cruz, P. (1989). *Formación y evolución de los derechos fundamentales, Revista española de Derecho Constitucional,* p. 41.

Do Amaral De Pauli, P. (2014). *Derechos de personalidad en las relaciones laborales y daño moral* [Tesis doctoral, Universidad de Burgos]. https://www.corteidh.or.cr/tablas/r38310.pdf

Estrada, J. (s.f.). *El derecho a la intimidad y su necesaria inclusión como garantía individual.* p.3 http://www.ordenjuridico.gob.mx/Congreso/pdf/86.pdf

Ferrajoli, L., Baccelli, L., Cabo, A. D., & Pisarello, G. (2001). *Los fundamentos de los derechos fundamentales,* 4th ed., pp.19-20.

Gonet, P. (2007). "Aspectos de Teoria Geral dos Direitos Fundamentais". En: Ferreira, G.,

Mártires, I., Gonet, P. *Hermenêutica constitucional e direitos fundamentais.* Brasília: Jurídica, p.107.

Guerrero, E. (2018). *El derecho al olvido digital en México,* pp.57-59. https://www.itei.org.mx/v3/micrositios/cdc/wpcontent/uploads/2020/04/7_2018_7_guerrero.pdf

Guerrero, Elvia. (2018). *El derecho al olvido digital en México,* p. 58 https://www.itei.org.mx/v3/micrositios/cdc/wp-content/uploads/2020/04/7_2018_7_guerrero.pdf

Johnson, N., et al. (2013) en Scherer, M. (2016) *Regulating artificial intelligence systems: risks, challenges, competencies, and strategies.* P. 366.

Kelly, M., Satola, D. (2017). T*he right to be forgotten, University of Illinois Law Review,* p.3 https://deliverypdf.ssrn.com/delivery.php? ID=635090098026019009092111103016030113035055008027063057097125085071104123123027115023103053058028021063113099028000120095009123118025036001009 1

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences,* Londres, Sage.

Landa, C. (2002). Teoría de los derechos fundamentales, cuestiones constitucionales, *Revista mexicana de Derecho Constitucional,* México, núm. 6, p.58. en: http://www.juridicas.unam.mx/publica/rev/cconst/cont/6/ard/ard3.htm

López, E. (2015). *El caso Google: lo que olvida el IFAI.* https://eljuegodelacorte.nexos.com.mx/el-caso-google-lo-que-olvida-el-ifai/

López, R. (2018). *La dignidad humana en México: su contenido esencial a partir de la jurisprudencia alemana y española.* P.152. http://www.scielo.org.mx/pdf/bmdc/v51n151/2448-4873-bmdc-51-151-135.pdf

Maciejewski, M. (2021). *La protección de los datos personales.* https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales#:~:text=El%20Convenio%20n.&text=108%20del%20Consejo%20de%20Europa,de%20la%20protecci%C3%B3n%20de%20datos.

MacMenemy, D. (2016). *Rights to privacy and freedom of expression in public libraries: squaring the circle.* https://pure.strath.ac.uk/ws/portalfiles/portal/54531639/McMenemy_IFLA_2016_rights_to_privacy_and_freedom_of_expression_in_public_libraries.pdf

Mantelero, A. (2018). *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review,* 34(4), 754-772. https://www.sciencedirect.com/science/article/pii/S0267364918302012?via%3Dihub

McKinsey Global Institute, (2015). *The internet of things: mapping the value beyond the hype,* p.38. https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-

value-beyond-the-hype.pdf

Muhila, V. (2008). *El derecho de acceso a la información como un derecho humano,* p.56. http://contraloriadelpoderlegislativo.gob.mx/Revista_Rc_et_Ratio/Rc_et_Ratio_1/Rc1_3_Victor_Muhlia_Melo.pdf

Nersessian, D. (2018). *The law and ethics of big data analytics: A new role for international human rights in the search for global standards. Business Horizons,* 845-854. https://www.sciencedirect.com/science/article/abs/pii/S0007681318301095

Nilsson, N. (2010). *The quest for artificial intelligence, A history of ideas and achievements, Stanford University,* p.13. https://ai.stanford.edu/~nilsson/QAI/qai.pdf

Organización de las Naciones Unidas. (2011). *Principios rectores sobre las empresas y los derechos humanos.* Puesta en práctica del marco de Naciones Unidas para "proteger, respetar y remediar. Nueva York, Ginebra: Oficina del Alto Comisionado para los Derechos Humanos. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

Pacto Internacional de Derechos Civiles y Políticos (1966). https://www.ohchr.org/documents/professionalinterest/ccpr_sp.pdf

Poudel, S. (2016). *Internet of Things: underlying technologies, interoperability, and threats to privacy and security,* Berkeley Technology Law Journal, pp. 997-1022.

Simitis, S. (1985) en Morozov, E. (2013). *The Real Privacy Problem*, párr. 16-18 https://www.technologyreview.com/2013/10/22/112778/the-real-privacy-problem/

Vecchio, G. (1968). *La déclaration des droits de l'homme et du citoyen dans la revolution française,* Roma, edition Fondation Européenne Dragan, p. 39.

Verceli, A. (s.f.) La (des)protección de los datos personales: análisis del caso Facebook Inc. - Cambridge Analytica, SID, Simposio Argentino de Informática y Derecho, pp.8-9. https://47jaiio.sadio.org.ar/sites/default/files/SID-1.PDF

Vladeck, D. (2014). Machines Without Principals: Liability Rules and Artificial Intelligence, 89 Wash. L. Rev. p.121.

Wylie, C. (s.f.) The Guardian (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election