DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

BIG DATA, BIG DATA ANALYTICS Y DATOS PERSONALES EN LOS TIEMPOS DEL INTERNET: DE LA AUTORREGULACIÓN ESTADOUNIDENSE AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

BIG DATA, BIG DATA ANALYTICS AND PERSONAL DATA IN THE INTERNET ERA: FROM THE AMERICAN AUTOREGULATION TO THE EUROPEAN UNION GENERAL REGULATION OF DATA PROTECTION

Mauricio Augusto CALCANEO MONTS*

RESUMEN: El artículo expone y explica las implicaciones derivadas del surgimiento y uso cada vez más extendido del internet, en términos de los datos personales de sus usuarios. En particular, se aborda lo relativo al impacto que tiene el *big data* o la existencia de grandes volúmenes de datos personales obtenidos a partir de los registros electrónicos, así como el procesamiento y análisis de dichos datos mediante el *big data analytics*. Para ello, se analizan los modelos regulatorios que existen sobre la materia en Estados Unidos y la Unión Europea, concluyéndose sobre la inviabilidad de la autorregulación norteamericana y la necesidad de enfoques más amplios, como el europeo.

PALABRAS CLAVE: Internet, *big data, big data analytics*, datos personales, regulación.

* Licenciado en derecho por la UNAM, licenciado en economía por la UAM-Xochimilco, maestro en derecho administrativo y regulación por el ITAM, y candidato a doctor por el Posgrado en Ciencias Políticas y Sociales de la UNAM. Correo: *calcaneomonts@yahoo.com*.

Fecha de recepción: 6 de junio de 2018.
Fecha de dictamen: 16 de marzo de 2019.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

ABSTRACT: The article exposes and explains the implications derived from the rise and increasingly widespread use of the internet, in terms of the personal data of its users. In particular, it deals with regard with the impact that big data has or the existence of large volumes of personal data obtained from electronic records, as well as the processing and analysis of such personal data through the big data analytics. In this regard, the regulatory models that exist in United States and in the European Union on the matter are analyzed, concluding on the unfeasibility of the American auto-regulation and the need for broader approaches as the European one.

KEY WORDS: Internet, big data, big data analytics, personal data, regulation.

I. Introducción

El Internet conecta a miles de millones de seres humanos prácticamente a todo lo largo y ancho del orbe, eliminando así las barreras espaciales y temporales existentes con antelación. Es, sin duda alguna, un cambio de gran calado en el ámbito tecnológico y de las comunicaciones, con hondas repercusiones sobre la forma en que los seres humanos interactúan y se comunican.

El éxito del Internet está sustentado en el tipo de comunicación que alberga, que es llevada a cabo en forma instantánea y de manera impersonal o indirecta a través de dispositivos electrónicos. Es gracias a esta mediación electrónica que se cuenta con registros en tiempo real de prácticamente la totalidad de las actividades efectuadas por los usuarios del Internet (Varian, 2010).

Es una cantidad ingente de información sobre los más diversos movimientos de todos y cada uno de los usuarios del Internet (*big data*), que ha sido posibilitada por el desarrollo acelerado y el consiguiente abatimiento de los costos de las tecnologías y técnicas atinentes a la recolección, almacenamiento y procesamiento de dicha información, lo que se ha visto acompañado por importantes progresos en las capacidades tecnológicas, técnicas y humanas para el análisis de la información (*big data analytics*) (Cate, 2014; Einav y Levin, 2013; White House, 2014a y 2014b; Federal Trade Commission, 2014).

Es decir, si bien el Internet ha hecho realidad una mayor y mejor comunicación entre individuos, al mismo tiempo, por su propia naturaleza

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

electrónica, ha permitido, por vez primera en la historia de la humanidad, la existencia de enormes volúmenes de información a un nivel de detalle sin precedentes sobre las actividades de sus usuarios, lo que, desde luego, no ha estado exento de una serie de cuestionamientos relacionados con la cantidad de información extraída, su contenido, la privacidad, y el uso que se está haciendo de esta información con propósitos analíticos y predictivos en los más distintos ámbitos de la actividad social (Kosinski y Behrend, 2017; Tucker *et al.*, 2017; Altman *et al.*, 2018; Tucker *et al.*, 2018).

Son dos los modelos regulatorios diametralmente opuestos en el ámbito de las democracias occidentales sobre los datos personales en el Internet: uno, el norteamericano, que es el más ampliamente extendido hasta ahora, y que se sustenta en la autorregulación de las empresas; el otro, el europeo, que reconoce una serie de derechos que protegen ampliamente los datos personales de los usuarios europeos del Internet, y que pone límites claros al actuar de las empresas (Wheeler, 2018), que pueden ser explicados con base en las diferencias culturales, políticas y jurídicas de ambos lados del Atlántico; la europea, más proclive a la intervención estatal, y la norteamericana, más cimentada en la libertad individual (Fukuyama, 2018).

El texto tiene como objetivo exponer y explicar la situación de los datos personales en los tiempos del Internet, los desafíos que esto implica y las medidas que en materia regulatoria se han tomado tanto en Estados Unidos como en Europa. En primer término, se aborda lo relacionado con el cúmulo de información disponible a partir del surgimiento y uso cada vez más extendido del Internet (*big data*), para después entrar al detalle de los avances técnicos y tecnológicos para el análisis de tales datos y su aplicación con fines explicativos, predictivos, e inclusive de manipulación (*big data analytics*). En segundo lugar, se revisan a la luz del marco analítico que proporcionan el *big data* y el *big data analytics*, los marcos regulatorios de los Estados Unidos y la Unión Europea relacionados con los datos personales en el Internet. El contraste es muy marcado, pues mientras en el primer caso, Estados Unidos, prevalece un esquema de autorregulación empresarial, en Europa, por el contrario, hay un reconocimiento de los derechos de los titulares de los datos personales y una fuerte regulación estatal sobre qué se puede recolectar, y sobre todo, qué se puede hacer con ellos. Se concluye que la regulación europea es, desde esta perspectiva, la respuesta más acorde a los desafíos que implican el *big data*, el *big data analytics* y los datos personales en los tiempos del Internet.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

II. *Big data, big data analytics* y datos personales

Conceptualmente, el *big data* se refiere a la existencia de una ingente cantidad de datos asociados al uso cada vez más extendido del Internet y los dispositivos electrónicos vinculados a éste, tales como las computadoras, los teléfonos celulares, las aplicaciones para dispositivos móviles, los geolocalizadores, los sensores, y otros (Cate, 2014).

Sobre la ingente cantidad de datos disponibles, baste destacar que para 1999 se hablada de una producción anual de nueva información de aproximadamente dos exabytes;[1] para 2002, dicha cantidad se había incrementado a cinco exabytes anuales correspondientes una tasa de crecimiento anual del 30% (Lyman y Varian, 2003), mientras que para 2013 se calculaba que se generaban los mismos cinco exabytes de información, pero cada dieciocho días (Einav y Levin, 2013). De forma que en 2013 se estimaba en cuatro zettabytes[2] el tamaño de la información generada.

No sólo es un enorme volumen de información disponible, sin parangón en la historia de la humanidad, sino que además se caracteriza por la velocidad en que puede ser obtenida, alcanzando incluso el tiempo real, por no hablar de su gran variedad al abarcar los más distintos aspectos de la actividad humana y a niveles de detalle nunca antes vistos. Como afirman Einav y Levin (2013: 2 y 3):

> Prácticamente en internet todo es registrado. Cuando haces una búsqueda en Google o Bing, tus preguntas y subsecuentes acciones son registradas. Cuando compras en Amazon o eBay, no sólo cada compra, sino tus siguientes acciones son capturadas y registradas. Cuando lees un periódico en línea, ves videos, o revisas tus finanzas personales, todo tu comportamiento es registrado. El registro del comportamiento individual no se limita al internet: los mensajes de texto, los teléfonos celulares y la geo-localización, los datos escaneados, los datos laborales, y los datos electrónicos de salud, todos son parte de una huella de datos que vamos dejando.

La Comisión Federal de Comercio de los Estados Unidos, por ejemplo, investigó el actuar de los llamados *data brokers*, o las "empresas que recolectan información personal de los consumidores y la revenden o comparten con otras compañías" (Federal Trade Commission, 2014). Los ha-

[1] Un exabyte (EB) es equivalente a 1,000,000,000,000,000,000 bytes o 1018 bytes. Un byte es igual a un carácter de texto.

[2] Un zettabyte es igual a 1,000,000,000,000,000,000,000 bytes o 1021 bytes.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

llazgos son reveladores con relación al tipo de información que se extrae, la forma en que se consigue y los usos que se le dan:

> 1) La información es obtenida vía internet y medios electrónicos asociados a éste, sin que los consumidores conozcan lo más mínimo sobre la existencia y operación de estas empresas, qué información recolectan ni cómo la procesan y usan.
>
> 2) La información de los consumidores con la que cuentan los *data brokers*, incluso indefinidamente, incluye nombres, direcciones, edad y registros de transacciones.
>
> 3) Los *data brokers* combinan estos datos para efectos de análisis y la realización de una serie de inferencias sobre los hábitos, gustos y demás aspectos relativos a los consumidores.
>
> 4) La información personal sobre los consumidores permite dar seguimiento puntual a cada uno de los mismos y es usada en una amplia variedad de industrias con tres fines principales: la publicidad personalizada en línea, la mitigación de riesgos y la búsqueda de productos.

Es un conjunto de información personal, profunda y vasta sobre quienes usan el Internet, que es obtenida y almacenada a partir de las posibilidades que brindan los desarrollos tecnológicos-computacionales, que han abatido los costos asociados a estas operaciones; que están en posesión de entes tales como los proveedores de servicios de telecomunicaciones, las redes sociales, las tiendas en línea, las empresas de telefonía celular, los bancos, los *data brokers*, los navegadores de Internet, los buscadores de información en Internet, y otros; y de la que se desconoce, en la gran mayoría de los casos, inclusive su propia existencia, por no hablar de su contenido preciso por parte de quienes son sus legítimos titulares (White House, 2014a y 2014b).Todo lo cual conlleva serias interrogantes en términos de la privacidad de los individuos y los datos personales de los usuarios del Internet.

La situación se torna todavía más crítica cuando se abordan los usos que se dan a esta información vía el *big data analytics* o, lo que es lo mismo, mediante el procesamiento y análisis del gran cúmulo de información disponible por medios electrónicos.

Si el *big data* se refiere a la gran cantidad de información de los individuos que se recopila, almacena y procesa a partir de la actividad de aquéllos en el Internet, el *big data analytics* trata del análisis de tal información para detectar patrones de comportamiento, los que son utilizados con fines predictivos, e incluso de modificación de los mismos (White House, 2014b).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

El *big data analytics* implica un gran salto cualitativo en términos de las capacidades tecnológicas, técnicas y humanas para trabajar y manipular ese enorme cúmulo de información conseguida a través de Internet, con el fin de obtener un orden, encontrar variables, patrones y relaciones, y no sólo eso, sino también poder anticipar comportamientos, e inclusive influir y moldear éstos en las más distintas esferas de la actividad humana (desde el simple acto de comprar un producto en Internet hasta hechos relacionados con elecciones de tipo político).

A través del *big data analytics* se crean modelos de comportamiento de los individuos, se realizan experimentos en tiempo real y se personaliza lo que ven y hacen en el Internet con base en su comportamiento previo (Varian, 2010).

La evidencia empírica sobre el *big data analytics* ha confirmado plenamente las múltiples posibilidades de su aplicación. Por ejemplo, en el contexto político se ha comprobado su utilidad lo mismo para movilizar votantes que para extraer información sobre las cualidades personales de los usuarios de Internet.

En un experimento realizado con motivo de las elecciones legislativas norteamericanas del 2 de noviembre de 2010, se incluyeron una serie de mensajes en Facebook para analizar si afectaban la autoexpresión política, la búsqueda de información y la emisión del voto. Los resultados son positivos para los tres efectos buscados; la movilización política en línea sí funciona para la inducción de estos tres tipos de conductas. Más importante todavía, la publicidad en Internet tiene influencia en los comportamientos de los individuos en la vida real (Bond *et al.*, 2012).

De igual manera, se comprobó que los "me gusta" en Facebook pueden servir para predecir con gran exactitud una serie de atributos personales de sus usuarios, como son las preferencias sexuales, el grupo étnico, la religión que se practica, los rasgos personales, la inteligencia, la felicidad, el uso de sustancias adictivas, la edad, el género, la separación de los papás y las preferencias políticas (Kosinski *et al.*, 2013).

La situación resultante es clara: un contado número de personas, empresas y gobiernos detentan la información y los conocimientos atinentes para acceder a profundidad, en forma detallada y en tiempo real, a las más variadas actividades de los individuos, para a través de esto predecir sus comportamientos, y, sobre todo, estar en aptitud de ejercer sobre ellos cierto tipo de influencia (White House, 2014). Es un poder sinigual en la historia del hombre, que se puede prestar a usos socialmente incorrectos, como lo es la manipulación de todo tipo, y que está cimentado en los datos personales de sujetos que en su mayoría desconocen dichos procesos.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

La experiencia de la elección presidencial norteamericana de 2016 es reveladora a este respecto:

Está ampliamente documentada y probada la intervención de Rusia en las elecciones presidenciales norteamericanas por conducto de las redes sociales, utilizando publicidad pagada, con alto contenido ideológico y cultural, y dirigida a sujetos con ciertas características particulares, que los hacían propensos a estos temas divisivos (Freedom House, 2017; Persily, 2017; Tucker *et al.*, 2017).

Los gigantes del Internet, como Facebook, Google y Twitter, han rendido testimonio sobre el tema ante los comités de las cámaras de senadores y de representantes de los Estados Unidos, e incluso ante los parlamentos europeo y británico. Facebook, por ejemplo, aceptó que más de 126 millones de personas fueron alcanzadas por la publicidad contratada por la denominada Agencia de Investigación de Internet, de origen ruso. Twitter informó que identificaron 3,814 cuentas vinculadas con la misma agencia, las que emitieron 175 mil "tuits", que significaron el 8.4% de los mensajes relacionados con la campaña presidencial norteamericana. La investigación periodística "Expedientes de *Cambridge Analytica*" documentó la sustracción, por parte de la empresa SCL Group/SCLElections/Cambridge Analytica, de los datos personales de las cuentas de Facebook de 87 millones de usuarios, en su mayoría estadounidenses, con el fin de crear perfiles psicológicos y políticos de los 230 millones de norteamericanos para su uso en la campaña presidencial de 2016, mediante diversas operaciones, que incluyeron rumores, desinformación y noticias falsas. Como consecuencia, el Departamento de Justicia estadounidense acusó formalmente a trece personas y tres compañías por el diseño de una red para subvertir las elecciones presidenciales de 2016, promover la discordia, socavar el respaldo público a la democracia y apoyar al ahora presidente de Estados Unidos.

Las redes sociales han ocupado un lugar privilegiado en la diseminación de información falsa, discursos de odio, interferencia electoral, propaganda extremista y con alto contenido conspirativo, que tiende a la polarización, entre otros. Como afirma Larry Diamond (2019), en un muy corto periodo de tiempo se pasó de una visión optimista de las redes sociales, como herramientas de la libertad de expresión y para el combate contra los gobiernos autoritarios, a otra francamente pesimista, por los efectos adversos que tiene en el funcionamiento de la democracia.

Frente a esta situación, son múltiples los llamados en Estados Unidos y alrededor del mundo para revisar y modificar el modelo de regulación imperante en materia de datos personales obtenidos en el Internet (Goldfarb y Tucker, 2011; Kosinski y Behrend, 2017; Altman *et al.*, 2018). Inclusive

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

Mark Zuckerberg, fundador y director ejecutivo de Facebook, se ha pronunciado recientemente en favor de cambiar la regulación norteamericana en la materia y transitar hacia un esquema similar al de la Unión Europea (Zuckerberg, 2019). En seguida, se exponen los pormenores del modelo de regulación norteamericano de datos personales hasta ahora vigente, para después proceder a contrastarlo con el de Europa.

III. La regulación norteamericana de datos personales en Internet

La regulación norteamericana sobre privacidad, datos personales y tecnologías de la información y comunicación se remonta por lo menos a fines del siglo XVIII, cuando se declaró ilegal la apertura de la correspondencia postal (1782). Desde entonces y hasta ahora se reconoce ampliamente la constante y cambiante relación y tensión que existe entre cambio tecnológico en el mundo de las telecomunicaciones y la vida privada de los individuos (Goldfarb y Tucker, 2011).

El primer antecedente se encuentra en la cuarta enmienda de la Declaración de Derechos de 1791, que protege básicamente los derechos a la privacidad y a no sufrir una invasión arbitraria, al establecer el

> derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias frente a allanamientos y registros arbitrarios será inviolable, y no se expedirá ningún mandamiento, sino en virtud de causa probable, apoyado en juramento o promesa, que describa el lugar que ha de ser registrado y las personas o cosas que han de ser detenidas o incautadas.

Sin embargo, es ampliamente reconocido que no fue hasta un siglo después, en 1890, con la publicación del artículo seminal "El derecho a la privacidad", de Warren y Brandeis, si bien referido al impacto negativo de las cámaras portátiles y las fotos en la privacidad de las personas, cuando se emprendieron los primeros pasos para incluir el aspecto electrónico en el derecho a la privacidad, cuando también se dio a luz al derecho a la privacidad entre las personas y con respecto al gobierno, y se pusieron los fundamentos para la responsabilidad civil por los daños ocasionados.

Posteriormente, hay una serie de desarrollos en el ámbito jurisdiccional, como lo es la opinión disidente de 1928 del juez de la Suprema Corte, Louis Brandeis, en el caso Olmstead contra los Estados Unidos, en el que se proclamó el derecho a estar solo contra la intervención del gobierno, lo que fue interpretado de la manera más amplia y abarcadora posible. En

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

1939, el tratado de jurisprudencia de expresión de agravios reconoció la invasión a la privacidad como base para el derecho de acción. Y en 1967, una nueva interpretación de la Corte Suprema en el caso Katz contra Estados Unidos estableció que las expectativas subjetivas de privacidad están protegidas cuando se consideran razonables.

Fue en las décadas de los setenta y ochenta del siglo pasado, con el surgimiento de las computadoras y de las grandes bases de datos, cuando se construyó en Estados Unidos el andamiaje jurídico vigente hasta la actualidad, sobre manejo de datos personales en ciertos sectores económicos y en las plataformas tecnológicas a ellos asociadas.

En 1970 se emitió la primera de las regulaciones sectoriales, la Ley de Información de Crédito Justo (Fair Credit Reporting Act o FCRA, por sus siglas en inglés), cuyo objetivo es, de conformidad con el apartado b) del artículo 602,

> exigir que las agencias de informes de consumidores adopten procedimientos razonables para satisfacer las necesidades de comercio de crédito al consumidor, personal, seguros y otra información de manera justa y equitativa para el consumidor, con respecto a la confidencialidad, exactitud, relevancia y uso adecuado de dicha información.

El año de 1973 fue crucial para los desarrollos futuros en materia de protección de la información de las personas en un entorno caracterizado por el uso cada vez más extensivo de las computadoras y los sistemas de registros vinculados a éstas. Es en tal año cuando, en un influyente reporte intitulado "Registros, Computadoras y los Derechos de los Ciudadanos" (*Records, Computers and the Rights of Citizens*), elaborado a instancias del Departamento de Salud, Educación y Bienestar, se enuncian los cinco Principios Prácticos de Información Justa (*Fair Information Practice Principles* o simplemente FIPPS, por sus siglas en inglés), y que se transcriben a continuación (Ohm, 2014: 97):

1. No debe haber sistemas de registro y posesión de datos personales cuya existencia sea secreta.
2. Debe haber una forma para que la persona sepa qué información sobre ella es registrada y cómo es usada.
3. Debe haber una manera para que la persona prevenga que la información obtenida sobre ella con un propósito sea usada o esté disponible para otros propósitos sin el consentimiento de la misma persona.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

4. Debe haber una manera para que una persona corrija o enmiende un registro de información acerca de ella.
5. La organización que genere, mantenga, use o propague registros identificables de datos personales debe asegurarse de la confiabilidad de los datos para el uso intentado, y debe tomar precauciones para prevenir usos inadecuados.

Son cinco principios concisos sobre la recopilación y uso de los datos personales en el amanecer de los tiempos de las computadoras, que, como se desprende de su lectura, implican que no debían existir sistemas secretos de registro y posesión de datos personales; posibilitan a las personas conocer cómo y para qué se usa su información; desautorizan el uso de la información para objetivos distintos a los que se plantearon al momento de su recolección; permiten la corrección o enmienda de los datos de las personas, y enuncian obligaciones de confiabilidad y prevención para las organizaciones que trabajen con estos datos.

Los cinco principios, no obstante, adolecieron de obligatoriedad, por lo que "en la práctica, con excepción de unos pocos sectores, como el del cuidado a la salud, el enfoque de los FIPPs en los Estados Unidos ha sido reducido a los procedimientos para asegurar el aviso y consentimiento" (Strandburg, 2014: 10). Su aplicación quedó entonces a merced de la autorregulación de los sectores económicos, lo que ha desembocado en un procedimiento de aviso, en la mayoría de los casos ininteligible, por parte de las empresas para recolección, almacenaje y procesamiento de los datos personales de los usuarios, y a un consentimiento de éstos bastante desinformado y limitado con relación a los datos que se recolectan y los usos que se darán éstas (White House, 2012; White House, 2014a y 2014b; Cate, 2014; Strandburg, 2014; Ohm, 2014).

Es posterior a los cinco Principios Prácticos de Información Justa que se emiten toda una serie de legislaciones, principalmente sectoriales, en materia de datos personales. En diciembre de 1974 se expidió la Ley de Privacidad (Privacy Act of 1974), con el fin de establecer restricciones y salvaguardas contra la invasión de la privacidad personal a través del uso indebido de datos y registros por parte de las agencias federales. La Ley define el término "registro" como

> cualquier artículo, recopilación o agrupación de información sobre un individuo que es mantenido por una agencia, incluyendo, pero no limitado a, su educación, transacciones financieras, historial médico y criminal o historial de empleo. Mientras que, en el apartado de condiciones de divulgación, se establece que "ninguna agencia divulgará registro alguno que esté contenido

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

> en un sistema de registros, por ningún medio de comunicación, a ninguna persona u otra agencia, excepto en virtud de una solicitud por escrito o con el consentimiento previo por escrito de la persona a quien el registro pertenece".

En el mismo 1974 se emitió la Ley de Privacidad y Derechos Educativos de la Familia (Family Educational Rights and Privacy Act o FERPA, por sus siglas en inglés), que regula la información personal relacionada con las escuelas, en específico los registros de los estudiantes; ya en la década de los noventa, en 1996, tocó el turno a la Ley de Responsabilidad y Portabilidad del Seguro de Salud (Health Insurance Portability and Accountability Act o HPAA, por sus siglas en inglés), que regula la información atinente a la industria de la salud; en 1998, entró en vigor la Ley de Protección de la Privacidad en Línea de los Niños (The Children's Online Privacy Protection Act o COPPA), que obliga a obtener el consentimiento de los padres para el caso de los servicios en línea dirigidos a los menores de trece años o que colectan datos de éstos; en 1999 se emitió la Ley Gramm-Leach-Bliley, que ordena a las instituciones financieras, respetar la privacidad, la seguridad y la confidencialidad de sus clientes.

Se trata de una serie de regulaciones que se caracterizan por (White House, 2014a y 2014b; Cate, 2014; Strandburg, 2014; Ohm, 2014):

1. Su enfoque eminentemente sectorial, que abarca de manera transversal al Internet en su conjunto, al ocuparse de sectores particulares, como son los de la salud, el crediticio y otros.
2. Sustentarse en el aviso y consentimiento como mecanismo para obtener el visto bueno de los usuarios para la recolección y procesamiento de sus datos, lo que conlleva problemáticas tales como la falta de capacidades de los usuarios para leer y asimilar los alcances e implicaciones de su consentimiento; la posibilidad de almacenar y usar la información obtenida por largos periodos de tiempo, e inclusive de manera indefinida, y el uso de la información con los más diversos fines y alcances.
3. Concentrarse en la recolección y revelación de la información más que en el uso que se dé a ésta, lo que conlleva a una situación en la que pretendidamente hay ciertos límites a lo que se puede recopilar y hacer público, y plena libertad en cuanto a cómo se utiliza dicha información, y
4. Todo lo cual da un amplio margen de autorregulación a las empresas que recolectan y procesan datos personales de los individuos en el Internet.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

Ante los retos que implican el *big data* y el *big data analytics* en términos de recolección y análisis del ingente y cada vez más detallado y preciso volumen de datos personales de los millones de usuarios del Internet, es patente que a estas alturas es insuficiente el modelo norteamericano de autorregulación sectorial de datos personales en el Internet.

A la fecha, son varios los intentos para que Estados Unidos cuente con una legislación transversal en materia de datos personales en el Internet: la propuesta de Ley de Derechos de Privacidad del Consumidor del presidente Obama de 2012; el llamado de 2014 de la Comisión Federal de Comercio para regular a los *data brokers*, y la regulación de "Protección de la Privacidad de los Clientes de Banda Ancha y Otros Servicios de Telecomunicaciones" de la Comisión Federal de Comunicaciones, que fue rechazada el 3 de abril de 2017 por una declaración conjunta del Congreso estadounidense (Ley Pública 115-22).

A nivel de los estados de la Unión Americana resalta el caso de California, donde se aprobó, el 25 de junio de 2018, la Ley de Privacidad del Consumidor, en vigor a partir del 1o. de enero de 2020. La que señala en el inciso *g)* de la sección 2, que "en marzo de 2018, salió a la luz que los datos personales de millones de personas habían sido mal utilizados por una empresa de extracción de datos llamada *Cambridge Analytica*... Como resultado, se ha fortalecido nuestro deseo de privacidad y transparencia en las prácticas asociadas a los datos...".

Por lo que la Ley de Privacidad otorga a los individuos el control sobre sus datos personales, mediante los siguientes derechos: saber qué información se está recolectando sobre ellos; si su información está siendo vendida o hecha pública, y a quién; tener acceso a su información, y negarse a que su información sea vendida.

Aparentemente, ni a la opinión pública ni a los tomadores de decisiones estadounidenses les basta ya con el modelo de autorregulación imperante de datos personales en el Internet. Existe lo que figura ser una fuerte corriente de opinión sobre la necesidad de regular el manejo de datos personales en Estados Unidos, aunque es difícil prever si esto llevará a un acuerdo sobre el tema y cuál será su contenido. Por ello, cobra especial relevancia lo que se está realizando en la Unión Europea mediante el Reglamento General de Protección Datos, cuestión que se aborda en el apartado siguiente.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

IV. El Reglamento General de Protección de Datos de la Unión Europea

En contraposición al modelo estadounidense de autorregulación sectorial de datos personales en el Internet, la Unión Europea cuenta desde el 25 de mayo de 2018 con el Reglamento General de Protección Datos, conforme al cual la privacidad es concebida como un derecho humano fundamental, por lo que se otorga una vigorosa protección en favor de los titulares de los datos personales, y ahora se está en presencia de una regulación transversal respaldada por una fuerte intervención estatal.

El caso europeo, al igual que el norteamericano, tiene una serie de antecedentes de larga data. El primero de ellos es el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales del Consejo de Europa de 1950, cuyo artículo 8 establece el derecho a la privacidad, al señalar que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".

No obstante, los primeros años de la década de los ochenta fueron cruciales en materia de protección de datos personales en el contexto de la expansión de las comunicaciones electrónicas, con la emisión de dos documentos con profundo impacto a futuro: las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980, y el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal de 1981.

Las Directrices de la OCDE de 1980 planteaban en su segunda parte ocho principios básicos de aplicación nacional, que a la letra señalan:

> Principio de limitación de recogida: Deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.
>
> Principio de calidad de los datos: Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.
>
> Principio de especificación del propósito: El propósito de la recogida de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

Principio de limitación de uso: No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el apartado 9, excepto si se tiene el consentimiento del sujeto implicado o por imposición legal o de las autoridades.

Principio de salvaguardia de la seguridad: Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos.

Principio de transparencia: Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

Principio de participación individual: Todo individuo tendrá derecho a: que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona; que se le comuniquen los datos relativos a su persona en un tiempo razonable; a un precio, si existiese, que no sea excesivo; de forma razonable; y de manera inteligible; que se le expliquen las razones por las que una petición suya según los subapartados (a) y (b) haya sido denegada, *así* como poder cuestionar tal denegación; y expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.

Principio de responsabilidad: Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Las Directrices de la OCDE de 1980 no tenían fuerza obligatoria y vinculante para los Estados. No obstante, fueron incluidos como parte sustantiva del Convenio 108 del Consejo de Europa, cuyo fin, según su artículo 1, es "garantizar… a cualquier persona física… el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal…". En los artículos 5 y 8 del Convenio se estableció lo que sigue:

Artículo 5. Calidad de los datos.

Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) Se obtendrán y tratarán leal y legalmente; b) Se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se haya registrado; d) Serán exactos y si fuera necesario puestos al día; e) Se conservarán bajo una forma que permita la identificación de las personas concernidas durante

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

el período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Artículo 8. Garantías complementarias para la persona concernida

Cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades… así como la identidad y residencia… de la autoridad controladora del fichero; b) Obtener… la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernen a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) Obtener… la rectificación de dichos datos o el borrado de los mismos…; d) Disponer de un recurso si no se ha atendido a una petición de confirmación o… de comunicación, de ratificación o de borrado.

Tanto las Directrices de la OCDE de 1980 como el Convenio 108 del Consejo de Europa contemplan una serie de disposiciones de suma importancia para el tratamiento de los datos personales en los tiempos de las comunicaciones electrónicas en al menos dos sentidos: reconocen una serie de derechos para las personas titulares de los datos personales, entre los que se encuentran los relativos a requerir su consentimiento, saber de su existencia, pedir su rectificación o eliminación, e interponer recursos de inconformidad, y garantizan el uso adecuado de los datos personales, al señalar límites para su recolección, los fines de ésta y las medidas de seguridad para el supuesto de pérdida o destrucción.

En 1995, en el contexto de la Unión Europea, se expidió la Directiva 95/46/EC del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, sobre la protección de los individuos con respecto al procesamiento de los datos personales y el libre movimiento de dichos datos, cuyo objeto es, acorde con su artículo 1, que los Estados miembros garanticen "la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales", y prohibir la restricción a "la libre circulación de datos personales entre los Estados miembros…".

Adicionalmente, la Directiva 95/46/EC contempló un conjunto de disposiciones a subrayarse: es aplicable al tratamiento automatizado y no automatizado de datos personales (artículo 3); los Estados miembros quedaron obligados a implementar en sus legislaciones nacionales las disposiciones de la Directiva (artículo 4); se estableció que los datos personales serían tratados de manera leal y lícita; recogidos con fines determinados, explícitos y legítimos, sin que sean tratados posteriormente de manera incompatible con dichos fines; adecuados, pertinentes y no excesivos; exactos y actualizados, y conservados en un periodo no superior al necesario

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

para cumplir con los fines de su recolección (artículo 6); se requirió que el tratamiento de los datos personales sólo pudiera efectuarse si el interesado daba su consentimiento de forma inequívoca (artículo 7); se obligó a los responsables del tratamiento de los datos a revelar su identidad e indicar los fines de la recolección (artículo 10); se reconoció el derecho de las personas titulares de los datos recabados a confirmar la existencia o inexistencia de los mismos, los fines de su uso, la rectificación, la supresión o el bloqueo de los datos (artículo 12); se contempló el derecho de oposición de las personas para el tratamiento de sus datos para su uso con fines de prospección (artículo 14); se obligó a los Estados miembros a establecer que toda persona disponía de un recurso judicial en caso de violación de sus derechos en esta materia y que hayan sido garantizados conforme a la normatividad nacional (artículo 22); se estableció que los Estados miembros dispondrían de autoridades públicas encargadas de vigilar la aplicación de la Directiva en su territorio (artículo 28), y se creó un grupo de protección de las personas en lo que respecta al tratamiento de datos personales (artículo 29).

La Directiva 95/46/EC ahonda en las medidas de protección de los datos personales contempladas en las Directrices de la OCDE de 1980 y en el Convenio 108 del Consejo de Europa, al incluir derechos tales como el de oposición y al recurso judicial, al tiempo de prever la existencia de autoridades públicas encargadas de la vigilancia de la aplicación de la Directiva en los Estados miembros.

El 27 de abril de 2016, el Parlamento y Consejo Europeo aprobaron el Reglamento General de Protección Datos de la Unión Europea, aplicable a partir del 25 de mayo de 2018. A diferencia de la Directiva 95/46/EC, el Reglamento no requiere de su traducción al ámbito nacional, sino que es aplicable de manera directa en todos los Estados, e inclusive en superiores jerárquicamente (Elias, 2014). Además, el Reglamento es una normatividad transversal, que protege fuertemente a los sujetos titulares de los datos personales, que pone límites a las actividades de quienes recaban y procesan dichos datos, y que implica una vigorosa intervención estatal. El Reglamento es un intento por poner al día la legislación en materia de datos personales con los desarrollos tecnológicos observados durante los últimos treinta años a raíz del surgimiento y uso cada vez más extendido del Internet.

El artículo 1 establece como objeto del Reglamento "la protección de las personas físicas en lo que respecta al tratamiento de los datos personales… [y la protección] de los derechos y libertades fundamentales de las personas físicas, y en particular, su derecho a la protección de los datos

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

personales". El artículo 3 se refiere a su ámbito territorial, al señalar que "se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento… independientemente de que el tratamiento tenga lugar en la Unión o no".

El artículo 5 versa sobre los principios relativos al tratamiento de los datos personales, al señalar que serán

> tratados de manera lícita, leal y transparente en relación con el interesado… recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines… adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados… exactos y, si fuera necesario, actualizados… mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

El artículo 6, por su parte, dispone que el tratamiento de los datos personales será lícito sólo si la persona da su consentimiento para tal efecto. De modo que el artículo 7 establece como condiciones para dicho consentimiento, que "el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales… la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo… el interesado tendrá derecho a retirar su consentimiento en cualquier momento…".

El artículo 13 desglosa la información que los responsables del tratamiento de los datos deberán proporcionar a los titulares de éstos, siendo las siguientes:

> La identidad y los datos de contacto del responsable… los fines del tratamiento de los datos personales… los destinatarios o las categorías de destinatarios de los datos personales… la intención del responsable de transferir datos personales a un tercer país u organización internacional… el plazo durante el cual se conservarán los datos personales… la existencia del derecho a solicitar el acceso a los datos personales y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos… el derecho a presentar una reclamación ante una autoridad de control… la existencia de decisiones automatizas, incluida la elaboración de perfiles…

El artículo 16 establece el derecho a la rectificación en caso de inexactitud en los datos personales. El artículo 17 contempla el derecho de

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

supresión o al olvido cuando los datos personales "ya no sean necesarios en relación a los fines para los que fueron recogidos o tratados… el interesado retire su consentimiento… [o] se oponga al tratamiento…". El artículo 18 se refiere al derecho a la limitación del tratamiento. El artículo 19 trata del derecho a la portabilidad de datos, que consiste en el derecho del interesado a "recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento". El artículo 21 regula el derecho de los interesados a oponerse a que los "datos personales que le conciernan sean objeto de un tratamiento".

El artículo 30 obliga a los responsables del tratamiento a llevar un registro de tales actividades. El artículo 32 les obliga a aplicar "medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo". Los artículos 33 y 34 obligan a los responsables del tratamiento a dar aviso a las autoridades y a los particulares, dentro de las 72 horas siguientes, en caso de violación de la seguridad de los datos personales. El artículo 35 instaura la evaluación de impacto relativa a la protección de datos cuando "sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías… entrañe un alto riesgo para los derechos y libertades de las personas".

El artículo 51 prevé la existencia de autoridades públicas independientes en cada Estado miembro, encargadas de "supervisar la aplicación del… Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión". El artículo 68 establece la creación del Comité Europeo de Protección de Datos como organismo de la Unión encargado de supervisar y garantizar la correcta aplicación del Reglamento, asesorar a la Comisión Europea en materia de datos personales, y emitir directrices, recomendaciones y buenas prácticas en el ámbito de los datos personales (artículo 70).

El artículo 77 prevé que "sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control". A su vez, el artículo 78 señala que "sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna".

El artículo 82 otorga el derecho a la indemnización y responsabilidad a "toda persona que haya sufrido daños y perjuicios materiales o inmateriales

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

como consecuencia de una infracción del… Reglamento". Mientras que el artículo 83 contempla las distintas multas administrativas aplicables por violaciones al Reglamento, las que tratándose de empresas pueden alcanzar el 4% del volumen de negocio total anual global del ejercicio financiero anterior.

En suma, el Reglamento actualiza a los desarrollos que han tenido lugar en los últimos treinta años, las disposiciones de la Unión Europea en materia de datos personales en el Internet. Es un punto de inflexión en la regulación sobre dicha materia al incluir disposiciones tales como su aplicación extraterritorial a quienes procesen datos de residentes europeos, independientemente de su localización; las condiciones para el otorgamiento del consentimiento para el tratamiento de los datos personales; los derechos de los titulares de los datos a la rectificación, al olvido, a la limitación del tratamiento, a la portabilidad, a oponerse al tratamiento, a la reclamación, a la tutela judicial efectiva y a la indemnización; las obligaciones de los responsables del tratamiento de datos, como es llevar un registro de las actividades de tratamiento, garantizar niveles adecuados de seguridad, dar aviso en caso de violaciones a la seguridad y hacer la evaluación de impacto para el uso de nuevas tecnologías; la creación de autoridades en la materia tanto a nivel nacional como comunitario, y la aplicación de multas administrativas por hasta el 4% del volumen de negocios globales de las empresas.

Las disposiciones del Reglamento han sido llevadas a nivel del derecho nacional de los países miembros de la Unión Europea, como es el caso de España y su Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, del 5 de diciembre de 2018. Su objeto es, acorde con el artículo 1, "adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo… relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones".

El Reglamento es, sin duda, un paso firme para fortalecer la protección del derecho de las personas sobre sus datos personales y el uso que de éstos se haga por terceros, y para inhibir y, en su defecto, sancionar de manera firme los comportamientos de las empresas que se aparten de las reglas establecidas para la obtención, almacenamiento, procesamiento y análisis de datos personales en el Internet.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

V. Conclusiones

Las preocupaciones sobre la privacidad y los datos personales en los tiempos del Internet abarcan el cada vez mayor volumen de información disponible sobre las personas y el nivel de detalle y profundidad alcanzado (*big data*), y, más importante, las crecientes capacidades en términos predictivos y su uso para intentar moldear los comportamientos humanos en las más distintas esferas de nuestra actividad (*big data analytics*).

A dicho respecto, son dos los grandes modelos de regulación que están vigentes en el ámbito de las democracias occidentales: el norteamericano y el europeo.

El modelo estadounidense de autorregulación empresarial está siendo cada vez más cuestionado, tanto desde el ámbito político como desde el académico y el ciudadano, por los grandes márgenes de discreción que se otorgan a las empresas en perjuicio de los individuos en aspectos tan medulares como los relativos a qué información personal se recolecta y cómo se usa ésta. Sin embargo, habida cuenta de la enorme polarización política prevaleciente en el vecino del norte, es poco probable que en el futuro cercano se tomen medidas a este respecto a pesar de las distintas propuestas existentes y de la presión cada vez mayor.

En Europa, la situación es diametralmente diferente, pues desde el 25 de mayo de 2018 está en vigor el Reglamento General de Datos Personales. Se trata, sin duda, de una regulación con un enfoque más acorde con la tradición jurídica romano-germánica y, por ende, más cercana a la cultura jurídica mexicana. Es una regulación con carácter obligatorio en los distintos Estados que integran a la Unión Europea, que abarca a la totalidad de los sectores involucrados, y que establece medidas en favor de los usuarios, como son los derechos al consentimiento expreso, a retractarse, al olvido, a la rectificación, a conocer qué datos tienen las empresas y cómo los usan, entre otros. Al tiempo que acota el actuar de las empresas mediante la posibilidad de aplicar sanciones de hasta el 4% de su volumen de negocios globales.

La regulación europea sobre datos personales en el Internet es, desde esta perspectiva, la respuesta más acorde a los desafíos que implican el *big data*, el *big data analytics* y los datos personales en los tiempos del Internet. Sin embargo, el debate no está cerrado ni mucho menos; por el contrario, hay toda una agenda de investigación por desarrollar, que comprende aspectos tales como el análisis minucioso de las distintas disposiciones de la regulación europea; los efectos a corto, mediano y largo plazos de su

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

entrada en vigor, tanto en el Internet como en las distintas industrias, en el *big data*, en el *big data analytics* y en la innovación tecnológica; la aplicación concreta de sus disposiciones tanto en el ámbito administrativo como en el jurisdiccional; el impacto que tendrá allende las fronteras sobre los distintos sistemas jurídicos y en los regímenes jurídicos nacionales, por mencionar sólo algunos. Tal es el reto en este tema de enorme incidencia y alcance para el presente y el futuro de nuestras sociedades.

VI. Fuentes

Altman, Micah *et al.*, 2018, "Practical Approaches to Big Data Privacy over Time", *International Data Privacy Law*, vol. 8.

Bond, Robert M. *et al.*, 2012, "A 61-Million-Person Experiment in Social Influence and Political Mobilization", *Nature*, vol. 489.

Cate, Fred H., 2014, "The Big Data Debate", *Science*, vol. 346.

Cubillos Vélez, Ángela, 2017, "La explotación de los datos personales por los gigantes del Internet", *Estudios en Derecho a la Información*, núm. 3.

Diamond, Larry, 2019, "The Threat of Postmodern Totalitarianism", *Journal of Democracy*, vol. 30.

Einav, Liran y Levin, Jonathan D., 2013, "The Data Revolution and Economic Analysis", *National Bureau of Economic Research Working Paper Series*, Working Paper 10635.

Elias, Peter, 2014, "A European Perspective on Research and Big Data Analysis", en Lane, Julia *et al.*, *Privacy, Big Data, and the Public Good*, Nueva York, Cambridge University Press.

Federal Trade Commission, 2014, *Data Brokers. A Call for Transparency and Accountability*, disponible en: *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf* (fecha de consulta: 17 de mayo de 2018).

Freedom House, 2017, *Freedom on the Net 2017. Manipulating Social Media to Undermine Democracy*, disponible en: *https://freedomhouse.org/report/freedom-net/freedom-net-2017* (fecha de consulta: 1o. de junio de 2018).

Fukuyama, Francis, 2018, "Facebook vs. Democracy. A Conversation with Francis Fukuyama", *Monday Note*, 14 de mayo, disponible en: *https://mondaynote.com/facebook-vs-democracy-a-conversation-with-francis-fukuyama-a01e513b9820* (fecha de consulta: 5 de junio de 2018).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

Goldfarb, Avi y Tucker, Catherine, 2011, "Privacy and Innovation", *National Bureau of Economic Research Working Paper Series*, Working Paper 17124.

Jain, Priyank *et al.*, 2016, "Big Data Privacy: a Technological Perspective and Review", *Journal of Big Data*.

Kosinski, Michal *et al.*, 2013, "Private Traits and Attributes are Predictable from Digital Records of Human Behavior", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 110, núm. 15.

Kosinski, Michal y Behrend, Tara, 2017, "Editorial Overview: Big Data in the Behavioral Sciences", *Current Opinion in Behavioral Sciences*, vol. 18.

Lazer, David *et al.*, 2009, "Computational Social Science", *Science*, vol. 323.

Lyman, Peter y Varian, Hal R., 2003, "How Much Information 2003?", disponible en: *http://groups.ischool.berkeley.edu/archive/how-much-info-2003/* (fecha de consulta: 15 de mayo de 2018).

Matz, Sandra C. *et al.,* 2017, "Using Big Data as a Window into Consumers' Psychology", *Current Opinion in Behavioral Sciences*, vol. 18.

Ohm, Paul, 2014, "Changing the Rules: General Principles for Data Use and Analysis", en Lane, Julia *et al., Privacy, Big Data, and the Public Good*, Nueva York, Cambridge University Press.

Pendergast, Tom, 2018, "The Next Cold War is Here, and It's All About Data", *Wired*, 28 de marzo, disponible en: *https://www.wired.com/story/opinion-new-data-cold-war/* (fecha de consulta: 12 de mayo de 2018).

Persily, Nathaniel, 2017, "Can Democracy Survive the Internet?", *Journal of Democracy*, vol. 28, núm. 2.

Shorey, Samantha y Howard, Philip N., 2016, "Automation, Big Data, and Politics: A Research Review", *International Journal of Communication*, núm. 10.

Strandburg, Katherine J., 2014, "Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Contest", en Lane, Julia *et al., Privacy, Big Data, and the Public Good*, Nueva York, Cambridge University Press.

Tucker, Joshua A. *et al.*, 2017, "From Liberation to Turmoil: Social Media and Democracy", *Journal of Democracy*, vol. 28, núm. 4.

Tucker, Joshua A., 2018, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, disponible en: *https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf* (fecha de consulta: 11 de junio de 2018).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

VARIAN, Hal R., 2010, "Computer Mediated Transactions", *American Economic Review: Papers and Preceedings*, núm. 100.

WHEELER, Tom, 2018, "Can Europe Lead on Privacy?", *New York Times*, 1o. de abril, disponible en: *https://www.nytimes.com/2018/04/01/opinion/europe-privacy-protections.html* (fecha de consulta: 12 de mayo de 2018).

WHITE HOUSE, 2012, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", *Journal of Privacy and Confidentiality*, núm. 2.

WHITE HOUSE, 2014a, *Big Data: Seizing Opportunities, Preserving Values*, Washington, D. C., Executive Office of the President, disponible en: *https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf* (fecha de consulta: 16 de mayo de 2018).

WHITE HOUSE, 2014b, *Big Data and Privacy: A Technological Perspective*, Washington, D. C., Executive Office of the President-President's Council of Advisors on Science and Technology, disponible en: *https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf* (fecha de consulta: 16 de mayo de 2018).

ZUCKERBERG, Mark, 2019, "The Internet Needs New Rules. Let's Start in these Four Areas", *The Washington Post*, 31 de marzo, disponible en: *https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.fbabc7d7beb7* (fecha de consulta: 1o. de abril de 2019).

Marco normativo

California Privacy Consumer Act, disponible en: *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375* (fecha de consulta: 12 de abril de 2019).

Constitución de los Estados Unidos de América, disponible en: *https://www.archives.gov/espanol/constitucion* (fecha de consulta: 12 de abril de 2019).

Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, disponible en: *https://www.coe.int/en/web/human-rights-convention/the-convention-in-1950* (fecha de consulta: 12 de abril de 2019).

Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Per-

DOI: http://dx.doi.org/10.22201/iij.25940082e.2019.8.13882

sonal del 28 de enero de 1981, disponible en: *http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf* (fecha de consulta: 13 de abril de 2019).

Directrices de la OCDE sobre Protección de la privacidad y flujos transfronterizos de datos personales de 1980, disponible en: *https://www.oecd.org/sti/ieconomy/15590267.pdf* (fecha de consulta: 13 de abril de 2019).

Directiva 95/46/EC del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, sobre la protección de los individuos con respecto al procesamientos de los datos personales y el libre movimiento de dichos datos, disponible en: *https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN* (fecha de consulta: 13 de abril de 2019).

Fair Credit Reporting Act, disponible en: *https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act* (fecha de consulta: 13 de abril de 2019).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, disponible en: *https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673* (fecha de consulta: 13 de abril de 2019).

Privacy Act of 1974, disponible en: *https://www.govinfo.gov/content/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf* (fecha de consulta: 13 de abril de 2019).

Reglamento General de Protección Datos de la Unión Europea, disponible en: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN* (fecha de consulta: 13 de abril de 2019).