Festín de datos

Empresas y datos personales en América Latina

Vivian Newman Pont
Daniel Ospina-Celis
Juan Carlos Upegui Mejía

DOCUMENTOS 58

Dejusticia
derecho · justicia · sociedad

DOCUMENTOS 58

Vivian Newman Pont Abogada de la Universidad Javeriana y licenciada en derecho por homologación en la Universidad de Barcelona, con posgrado en derecho administrativo (D.S.U.), Magíster (D.E.A.) en Derecho Público Interno de la Universidad de Paris II Panthéon-Assas y en Cooperación y Desarrollo de la Universidad de Barcelona. Actualmente se desempeña como directora de Dejusticia.

Daniel Ospina-Celis Abogado de la Universidad de los Andes e investigador de Dejusticia.

Juan Carlos Upegui Mejía Abogado y profesor titular de la Universidad Externado de Colombia, Doctor en Derecho por la Universidad Nacional Autónoma de México (UNAM). Investigador de Dejusticia.

Festín de datos

Empresas y datos personales en América Latina

Vivian Newman Pont
Daniel Ospina-Celis
Juan Carlos Upegui Mejía

Dejusticia
derecho · justicia · sociedad

Documentos Dejusticia 58
FESTÍN DE DATOS
Empresas y datos personales en América Latina

Varios autores.
Edición a cargo de: Vivian Newman Pont, Daniel Ospina-Celis y Juan Carlos Upegui
Festín de datos. Empresas y datos personales en América Latina. -- Bogotá: Editorial Dejusticia, 2020.
204 páginas: gráficas; 24 cm. -- (Documentos; 58)
ISBN 978-958-5597-31-0
1. Protección de datos personales 2. empresas y derechos humanos 3. privacidad 4. tecnología y derechos humanos - América Latina. I. Tít. II. Serie.

ISBN: 978-958-5597-32-7 Versión digital
978-958-5597-31-0 Versión impresa

Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia
Calle 35 Nº 24-31, Bogotá, D.C.
Teléfono: (57 1) 608 3605
Correo electrónico: info@dejusticia.org
https://www.dejusticia.org

Revisión de textos: Alejandra Torrijos M.
Preprensa: Precolombi EU, David Reyes
Cubierta: Lina Moreno
Impresión: Ediciones Antropos Ltda.
Bogotá, mayo de 2020

Contenido

Agradecimientos

Esta investigación es el resultado del concurso de muchas voluntades, personales e institucionales.

En primer lugar, queremos agradecer a nuestros aliados de Coding Rights en Brasil, de Derechos Digitales en Chile y de la Red en Defensa de los Derechos Digitales (R3D) en México, y en especial a los y las autoras de los capítulos por país: a Joana Varon, Bruna Martins dos Santos y Kimberly Anastácio, por Brasil, Paloma Herrera y Pablo Viollier, por Chile y a Milan Trnka Osorio, por México, y a todas las personas que aportaron su experiencia para mejorar los informes de sus respectivos países. Su trabajo comprometido durante el segundo semestre de 2019 nos dio los insumos para la comparación, para las recomendaciones de cierre y para la consolidación final del libro.

Queremos agradecer igualmente a nuestros colegas de Dejusticia que asistieron al seminario de discusión y comentaron el primer borrador completo de este libro. Sus comentarios y recomendaciones hicieron que el texto mejorara notablemente. El apoyo y acompañamiento de Celso Bessa y de Víctor Saavedra también fue fundamental, sobre todo para aliviar las imprecisiones en el uso de expresiones técnicas que suelen estar más allá del alcance de los legos. A María Paula Ángel, por la idea original del proyecto y por su atenta revisión del capítulo de Colombia y del estudio comparado. Asimismo, merece nuestra gratitud el equipo administrativo de Dejusticia, por su apoyo y compromiso diarios, de entre todos, agradecemos especialmente a Claudia Luque por su inestimable colaboración en el proceso editorial.

Asimismo, agradecemos a Alejandro Londoño y Sarah Osma de la Delegatura para la protección de datos, a Jonathan Bock y Luisa Isaza de la Fundación para la Libertad de Prensa, a Lucía Camacho de la

Fundación Karisma, a Ailidh Callander de Privacy International y a José Alejandro Bermúdez, consultor y experto, por asistir a nuestro grupo focal y ofrecernos su tiempo, su visión crítica y sus valiosos comentarios sobre el borrador del texto. También agradecemos a Nelson Remolina, actual delegado para la protección de datos en Colombia, por su interés en esta investigación y por su disposición a compartir sus puntos de vista.

Por último, y con una mención especial, queremos agradecer a Wellspring, nuestro financiador internacional, sin cuyo apoyo no hubiéramos podido terminar los trabajos de comparación, de armado y de edición final de este documento.

Introducción

1. Economía digital y big data

La tecnología, en general, y las tecnologías de la información y comunicación (TIC), en particular, han modificado el mundo en que vivimos. Los desarrollos tecnológicos recientes han impulsado cambios de paradigma en distintas áreas del saber y en la forma de relacionarnos con el entorno. La facilidad de acceder a dispositivos tecnológicos móviles (teléfonos inteligentes, tabletas, computadores portátiles, etc.) ha cambiado la forma en que interactuamos con la tecnología. Según un estudio realizado por GSMA, una asociación mundial de operadores móviles, la penetración de teléfonos inteligentes alcanzó a mediados de 2018 al 66 % de la población mundial y al 85 % de la población del Norte Global (GSMA 2018). Vivimos en una sociedad tecnológica en la que la mayoría de la población usa diariamente un dispositivo móvil.

Los desarrollos tecnológicos recientes, la evolución de internet y la interconectividad de los dispositivos han llevado a algunos a afirmar que nos encontramos en una cuarta revolución industrial. Teniendo en cuenta las posibilidades para el comercio que ofrece la tecnificación y digitalización del mundo, en 2011 el gobierno alemán lanzó la iniciativa Industria 4.0 (Industry 4.0). El objetivo de este programa era impulsar la manufactura digital por medio de la promoción de la digitalización e interconexión de productos, cadenas de valor y modelos de mercado (Comisión Europea 2017). En el marco de esta iniciativa, "los modelos de negocios basados en datos se convertirán en la mayor fuerza motriz de la Industria 4.0 en el futuro" (Comisión Europea 2017, 7). Si bien el programa alemán fue innovador en su momento —tanto que hoy en día el término 'Industry 4.0' es utilizado en la academia y en el mundo

empresarial—, lo cierto es que en 2020 ya no parece descabellado suponer que la digitalización y los datos son elementos comunes en la industria y sociedad moderna.

Esta revolución digital se caracteriza, asimismo, por la utilización de sistemas híbridos de producción ('cyber physical systems') basados en la integración de datos y conocimiento (Lu 2017). Lo anterior permite satisfacer las necesidades individuales de cada uno de los usuarios/clientes, crear un sistema de producción más eficiente, mejorar la relación entre el destinatario final y el productor o distribuidor e integrar y automatizar el mercado (Vaidya Ambad y Bhosle 2018). Dentro de la cuarta revolución industrial, el uso de datos desempeña un rol preponderante. Como lo afirma el Boston Consulting Group, "la colección y evaluación comprehensiva de datos de distintas fuentes" optimiza la producción, ahorra energía y se convertirá en el sustento básico para la toma de decisiones en tiempo real (2015, 5).

Las TIC recolectan y generan datos digitales gracias a internet, las redes sociales, nuestros dispositivos móviles, las aplicaciones que descargamos en ellos, y a muchas otras interacciones digitales que componen el día a día de gran cantidad de personas. Todos estos datos tienen gran valor para quien sepa y pueda analizarlos. Mediante los datos de una persona se puede inferir, por ejemplo, qué tipo de música le gusta, si tiene un hijo recién nacido o cuál es su corriente política. Esta información es valiosa comercialmente, pues permite, solo por mencionar uno de sus usos más inofensivos, ofrecer publicidad personalizada. Por tal motivo, hoy en día existen miles de empresas que recolectan, procesan, analizan o comercializan datos digitales. Precisamente, por eso se habla de una revolución industrial basada, en gran medida, en el uso masivo de datos.

El valor económico de los datos y las posibilidades que surgen para la industria de su correcta explotación han llevado a que miles de empresas busquen ingresar a dicho mercado. A estas compañías se les ha denominado 'empresas con modelos de negocios basados en datos' (EMNBD) porque realizan análisis o recolección de datos, venden productos o servicios que se basan en datos como su fuente principal, y/o los datos son un recurso valioso dentro de su modelo de negocio (Hartmann, Zaki, Feldman y Neely 2014, 6). Aunque existan distintas clasificaciones de las EMNBD —dependiendo, en parte, del uso específico dado a los datos—, es común la preponderancia que tiene el tratamiento de datos de terceros en su actividad comercial, bien sea por su comercialización directa, por

su uso en la segmentación de clientes/usuarios, optimización del servicio o de fidelización de la clientela.

La economía digital y la cuarta revolución industrial giran en torno al uso y análisis masivo de datos. En este contexto, cobra relevancia el *big data*, entendido como "los activos de información caracterizados por un volumen, una velocidad y una variedad tan elevados como para requerir tecnología específica y métodos analíticos para su transformación en valor" (De Mauro, Greco y Grimaldi 2014, 8). La definición de *big data* sobre la que existe cierto consenso implica que los datos se analizan interrelacionando tres elementos: 1) la variedad de los datos, 2) su volumen y 3) la velocidad con la que cambia la información (Elgendy y Elragal 2014). Lo anterior, sin embargo, no obsta para que algunos analistas incluyan elementos adicionales como la complejidad de los datos (Pence 2014).

No en vano, se ha considerado a los datos, especialmente gracias al análisis que permite el *big data*, como uno de los activos más importantes de la economía del siglo XXI. Esto se debe, entre muchas razones, a que, si bien los datos son atribuibles a las personas, quien obtiene provecho económico de su explotación es un tercero —usualmente una empresa— al agruparlos y analizarlos. En palabras de Michael Haupt (2016), los datos son un recurso creado por y para seres humanos soberanos, por lo que no podemos permitir que "un nuevo tipo de industrias extraigan valor de nosotros, como hemos hecho en el pasado" con otros recursos, sin que en este proceso haya una participación efectiva de los titulares de los datos, una regulación adecuada y unas prácticas de rendición de cuentas de las empresas que amasan estos datos y acrecientan con ello su poder.

Aunque la recolección y análisis de datos digitales parezca distante, lo cierto es que, al descargar cualquier aplicación en un dispositivo móvil, la empresa dueña de dicha aplicación usualmente tiene acceso a gran cantidad de datos almacenados en nuestros dispositivos, dependiendo de lo estipulado en su política de privacidad. Por ejemplo, es posible que la empresa tenga acceso a las fotos que tenemos guardadas, al listado de contactos, a nuestros datos de localización, a información básica sobre el dispositivo desde el que nos conectamos e incluso al porcentaje de batería que tenemos. Por eso,

> El desarrollo de la economía digital y del *big data* plantea desafíos importantes para los derechos a la intimidad y a la protección de datos personales de las personas, así como para la transparencia,

la seguridad de los datos y el derecho a la igualdad (Newman y Ángel 2019, 13).

En ese orden de ideas, resulta necesario mitigar los riesgos creados por las nuevas prácticas de tratamiento de datos personales y las alternativas que permite el *big data*, con el fin de garantizar los derechos humanos en el mundo digital[1].

El Grupo de Trabajo del Artículo 29, una iniciativa del Parlamento Europeo que desde 2018 funciona bajo el nombre de Comité Europeo de Protección de Datos, ha identificado que el análisis en masa de grandes cantidades de datos o *big data* genera distintos riesgos o preocupaciones. Para este grupo de expertos, el *big data* supone nuevos desafíos de cara a la protección de la privacidad en al menos los siguientes temas: 1) la escala a la que se recolectan los datos y la posibilidad de crear perfiles detallados de las personas, 2) la seguridad de los datos, 3) la transparencia con la que se deben manejar los sistemas de tratamiento de datos para permitir que las personas entiendan y controlen lo que sucede con su información personal, 4) la posibilidad de ser sometido a arbitrariedades o discriminación injustificada y 5) el aumento de la vigilancia estatal representada en un control masivo de la información de todos los ciudadanos (Grupo de Trabajo del Artículo 29 2013, 45).

Algunos entusiastas de la tecnología afirman que uno de sus mayores beneficios es su total imparcialidad frente a las personas, lo cual puede llevar a una mejor y más justa distribución de recursos. Aunque esto puede ser cierto, el *big data* y los algoritmos pueden, muchas veces, reproducir los sesgos sociales y por tal motivo crear discriminación o aumentar la desigualdad. En un reconocido artículo, Barocas y Selbst (2016) discuten cómo el uso de *big data* genera "un impacto dispar" en el acceso al empleo. Este impacto, aunque es muy similar a la discriminación, se diferencia de esta porque (al menos en criterio de los autores) no es posible probar un deseo activo de generar discriminación[2]. En esa misma línea, otros autores han argumentado que los algoritmos utilizados

---

1 Para una comprensión de la discusión sobre el uso de la tecnología y el *big data* en la creación de identidades digitales y la garantía de los derechos humanos, se puede ver el trabajo de Beduschi (2019).

2 Este argumento fue recogido por el profesor Frederik Zuiderveen Borgesius (2018) en su estudio para el Consejo de Europa (una de las organizaciones de derechos humanos más grandes del continente).

para el tratamiento de datos personales, por ejemplo, pueden ser abiertamente discriminatorios si no se usan adecuadamente —mejor dicho, si no existe transparencia total en su diseño y aplicación— y se mitigan sus riesgos (Kleinberg, Ludwing, Mullainathan y Sunstein 2018). Por tal motivo, y con el fin de evitar injusticias producto del uso inadecuado de la tecnología (especialmente de la inteligencia artificial), la lucha por la "transparencia algorítmica" ha tomado fuerza en los últimos años.

En adición, la recolección de grandes cantidades de datos permite que las empresas realicen *profiling* o creación de perfiles de las personas. Estos perfiles le son útiles a las EMNBD, en tanto permiten determinar a qué productos o servicios tiene acceso un grupo de personas o qué información se les muestra. Esto depende, en general, de los 'rasgos' que se extraen o derivan de la conducta en línea de las personas. El perfilamiento se realiza, usualmente, con fines comerciales, como ofrecer publicidad dirigida de acuerdo con los gustos de cada quien. Pero sus usos se pueden diversificar para avanzar distintas agendas ideológicas, políticas, religiosas o comerciales. Las prácticas de perfilamiento pueden causar discriminación —en tanto solo se le ofrece un cierto contenido a solo cierto tipo de personas—, pueden también afectar los derechos de libertad —mediante la inducción a realizar ciertas conductas y a modificar el comportamiento en la web— y pueden tener otros impactos, todavía no suficientemente explorados, sobre el comportamiento de las personas y los derechos humanos.

2. El problema de la regulación

Es innegable la importancia económica que tiene el uso y análisis de datos para la economía digital —que hoy en día es una economía global transnacional—. También es innegable que la recolección masiva de datos personales, mediante internet y de dispositivos móviles, supone grandes riesgos para la sociedad y para los derechos humanos en la era digital. Así las cosas, resulta necesario regular de alguna forma la recolección, uso, análisis y tratamiento de datos personales que hacen las EMNBD con el fin de salvaguardar los derechos a la protección de datos, a la privacidad y a la igualdad, entre otros.

Sin embargo, regular el tratamiento de datos personales por EMNBD en el escenario digital no es tarea fácil. Esto es así por varios motivos. En primer lugar, debido a la dinámica comercial transnacional de

las grandes empresas de internet como Google, Amazon, Facebook, Apple y Microsoft (GAFAM) la protección de datos "ya no es un tema de carácter nacional", sino que debe pensarse como una situación que supera fronteras (Culik 2018, 29). En segundo lugar, está su fabuloso poder económico. Según el portal Fortune 500, el valor de mercado de Microsoft el 29 de marzo de 2019 se aproximaba a los 900 000 millones de dólares[3]. Este valor supera con creces el PIB de varios países de renta media, incluyendo Colombia, el cual según cifras del Banco Mundial fue de aproximadamente 330 000 millones de dólares en 2018[4], casi la tercera parte del valor comercial de Microsoft. Aunque se trate de un ejemplo ilustrativo, el desbalance económico entre un actor y otro sí dificulta la regulación efectiva de la actividad comercial. En palabras de Todorov, "frente al poder económico desmesurado que detentan los individuos o los grupos de individuos que disponen de inmensos capitales, el poder político [nacional] suele resultar demasiado débil" (2012, 98). A esto se suma, además, que las empresas que hacen presencia en múltiples países deban adecuar una práctica que se replica a nivel mundial (el tratamiento de datos personales) a las legislaciones únicas y específicas de cada país, y no a una legislación mundial o al menos regional —fenómeno que se conoce como el problema de la fragmentariedad—. Esta situación dificulta que las EMNBD de carácter transnacional adapten sus prácticas de tratamiento de datos a las particularidades de la legislación nacional de los países en los que hacen presencia.

Por otro lado, el carácter transnacional de varias EMNBD dificulta su rendición de cuentas a nivel nacional. A partir de las reglas tradicionales de la aplicación territorial de la ley, el ordenamiento jurídico doméstico no suele reconocer competencia sobre el actuar de compañías con domicilio en otros países, y estas a su vez son reacias a responder en foros formalmente 'extraterritoriales'. Como se presentará en el cuerpo del presente libro, no es clara la competencia de las autoridades de protección de datos a nivel nacional sobre el actuar de las empresas que realizan tratamiento de datos de sus nacionales, pero cuya casa matriz y/o asiento efectivo se encuentra en otra nación —usualmente del Norte

3 Búsqueda generada en la página web del portal Fortune: https://fortune.com/fortune500/2019/search/?mktval=desc&sector=Technology

4 Búsqueda generada en la página web del banco: https://datos.bancomundial.org/pais/colombia

Global—. En la práctica, las EMNBD aducen este argumento cuando alguna autoridad, ya sea administrativa o judicial, intenta hacerlas rendir cuentas por su actuar[5].

Otro de los motivos por los que no resulta sencillo regular adecuadamente el tratamiento de datos personales que realizan las EMNBD —o el *big data* en general— es la complejidad técnica del tema y, por ende, el gran nivel de detalle requerido para que la regulación sea satisfactoria. Como se demostrará en los capítulos posteriores, no es suficiente en la era digital expedir normas generales sobre la protección de datos si estas o su interpretación no se ajustan a la realidad técnica del *big data* y a las diferentes formas de recolección, uso y análisis de datos que permiten los sistemas informáticos. Así las cosas, tanto el legislador como los intérpretes de la ley deben abordar (idealmente también conocer y entender) situaciones como la recolección de metadatos, el uso de *cookies*, la interoperabilidad de sistemas y bases de datos, las decisiones automatizadas y el mercado de datos.

3. Dos regulaciones relevantes: Europa y California

Teniendo en cuenta los riesgos que tiene la recolección masiva y el posterior análisis de datos personales en la era digital por parte de EMNBD, tanto la Unión Europea como el Estado de California (Estados Unidos) emitieron respectivamente normativas de protección de datos ajustadas a la era digital. Estas regulaciones son dignas de mención porque pretenden superar algunos de los problemas y/o limitaciones descritos en el apartado anterior y proteger los derechos de los usuarios de servicios o plataformas digitales.

---

5 Al respecto, vale la pena destacar los argumentos de Google LLC y Google Colombia Ltda., en la solicitud de nulidad de la sentencia T-063A de 2017 en la que la Corte Constitucional le ordenaba a la primera retirar un contenido de la plataforma www.blogger.com. En esta, Google LLC argumentó que la Corte Constitucional colombiana no tenía competencia para ordenarle retirar un contenido, entre otras porque Google LLC no tiene presencia física en Colombia, pues sus servicios son prestados de manera remota mediante internet. A pesar de que esta sentencia fue anulada mediante Auto 258 de 2018 y el caso fue finalmente resuelto mediante la Sentencia SU-420 de 2019, en el entretanto Google decidió acatar la orden judicial y retiró el blog sobre el que versó la controversia (Sentencia SU-420 de 2019).

El 27 de abril de 2016, el Parlamento europeo y el Consejo de la Unión Europea aprobaron el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) —Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo— (Unión Europea 2016). Este Reglamento entró en vigencia el 25 de mayo de 2018 y actualizó la normativa de protección de datos europea a las dinámicas propias de la era digital. El Reglamento reconoce explícitamente que "la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales" en tanto "la magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa" (GDPR, consideración 6). Es importante resaltar que el GDPR es aplicable al tratamiento de datos personales de residentes de la Unión Europea, incluso si el responsable (EMNBD) se encuentra por fuera de la UE, siempre que el tratamiento se relacione con la oferta de bienes y servicios (Artículo 3). También vale la pena mencionar que el GDPR regula extensamente el consentimiento otorgado por los usuarios —tanto que permite su retiro— (Artículo 7) y le otorga derechos como el de portabilidad (Artículo 20) y el de oposición (Artículo 21), mientras que le impone altas cargas de transparencia a quien realice el tratamiento de datos (Artículos 12 a 14).

La regulación europea es relevante para nuestro análisis, al menos por dos motivos. En primer lugar, porque se trata de una normativa regional que pretende balancear el poder económico de los operadores comerciales que realizan tratamiento de datos personales (EMNBD) con el poder político de la Unión Europea. En ese sentido, tiene vocación de ser acatada por las empresas en tanto no es un esfuerzo aislado de un país por regular el *big data*, sino de un conjunto de naciones que representa una parte significativa del mercado de datos y de la economía digital mundial. En segundo lugar, porque el GDPR se encuentra ajustado a la realidad técnica de la era digital y, por tal motivo, regula aspectos propios del tratamiento de datos en el siglo XXI que otras regulaciones (anteriores) ignoran. Lo anterior, en todo caso, no quiere decir que sea una regulación que deba ser emulada letra por letra por los Estados latinoamericanos, pero sí que constituye un referente o un punto de comparación para las legislaciones nacionales actuales y futuras de los países de la región.

Ahora bien, la territorialidad de la ley de protección de datos y su alcance ante empresas transnacionales también es un tema de interés en

el ámbito europeo. Recientemente, en septiembre de 2019, el Tribunal de Justicia de la Unión Europea estableció que del GDPR no se desprende que "los derechos consagrados en estas disposiciones [tengan] un alcance que vaya más allá del territorio de los Estados miembros". En ese sentido, el Tribunal concluye que, según la normativa europea, no se le puede exigir a Google que retire un contenido si este se encuentra en una versión nacional del motor de búsqueda que no haga parte de la Unión Europea (Unión Europea 2019).

Por otro lado, inspirándose en parte en el GDPR, el Estado de California (Estados Unidos) promulgó en 2018 la Ley AB-375, que modifica el Código Civil de California, también denominada Ley de Privacidad del Consumidor de California (*California Consumer Privacy Act,* CCPA, por sus siglas en inglés). Esta ley, que entró en vigencia el primero de enero de 2020, actualizó el régimen de protección de datos estatal a las dinámicas propias de la era digital y reconoció, entre otros, el derecho del consumidor a saber qué información personal es recolectada por las EMNBD (Sección 1.798.110) y a oponerse a la venta de sus datos personales (Sección 1.798.120).

A pesar de no tratarse de una normativa de carácter nacional en Estados Unidos, el CCPA puede tener un impacto similar al GDPR debido a que, al ser una regulación del Estado de California, "su población y el gran tamaño de su economía otorgan a sus leyes una influencia considerable en el resto del país" (Newman y Ángel 2019, 15). Otro elemento por resaltar es el hecho de que varias de las grandes empresas de internet a nivel mundial tienen su sede en California. Esto supone, de manera ilustrativa, que el CCPA le aplica territorialmente a EMNBD como Facebook (ubicada en Menlo Park, California), Google (ubicada en Mountain View, California), Apple (ubicada en Cupertino, California), Netflix (ubicada en Los Gatos, California) y Twitter (ubicada en San Francisco, California), por solo mencionar algunas.

4. Insumos para la regulación en América Latina

En el ámbito regional, si bien aún no existe una norma internacional de carácter vinculante sobre la protección de datos, hay dos foros que han avanzado estas discusiones. Por un lado, está la institucionalidad de la Organización de los Estados Americanos (OEA), en donde, por encargo de la Asamblea General, se han adelantado consultas al respecto en los

Estados miembros y se han producido algunos informes, a cargo del Departamento de Derecho Internacional y del Comité Jurídico Interamericano.

Por otro lado, está la Red Iberoamericana de Protección de Datos —compuesta por las autoridades de protección de datos de más de 13 países—. En el contexto de esta Red, se aprobaron en 2017 los *Estándares de protección de datos personales para los Estados iberoamericanos* (Red Iberoamericana de Protección de Datos 2019). A pesar de tratarse de un instrumento de *soft law*, estos Estándares son relevantes al menos por dos motivos: 1) porque sirven como patrón de referencia común para los Estados de la región; y 2) porque uno de sus objetivos principales es el tratamiento de datos personales en la era digital. Este objetivo es explícito en el Artículo 1.º, según el cual, los Estándares pretenden elevar el nivel de protección de las personas físicas, en lo que respecta al tratamiento de sus datos personales, teniendo en cuenta las exigencias que "demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana".

Estos Estándares incorporan cláusulas de gran importancia para el tratamiento de datos personales en la era digital, como la aplicación extraterritorial de sus disposiciones, cuando el encargado o responsable de tratamiento no se encuentre establecido en el territorio de algún país iberoamericano, pero las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a residentes iberoamericanos (Artículo 5.1). Además, se trata de un instrumento jurídico de textura abierta, debido a la gran cantidad de principios que incorpora (Artículos 10 a 23). Asimismo, reconoce los derechos de acceso (Artículo 25), rectificación (Artículo 26), cancelación (Artículo 27) y oposición —especialmente si el tratamiento tiene como objeto la mercadotecnia o la elaboración de perfiles— (Artículo 28). Por último, resaltamos que los Estándares garantizan el derecho de las personas físicas a no ser objeto de decisiones automatizadas que produzcan efectos jurídicos o similares cuando no medie intervención humana (Artículo 29).

5. Metodología y estructura del libro

Este libro nace de la pregunta sobre la idoneidad de la regulación de datos personales en cuatro países de América Latina —Brasil, Chile,

Colombia y México— para enfrentar los desafíos del tratamiento de datos en la era digital y sobre la existencia de mecanismos para hacer rendir cuentas a las EMNBD. Esta pregunta incluye otras, más específicas, sobre las prácticas de tratamiento de datos de las EMNBD, el equipamiento de los órganos nacionales de protección de datos para garantizar los derechos de los titulares de los datos personales y la necesidad (o no) de una regulación regional a nivel de América Latina sobre la protección de datos personales en la era digital.

Elegimos los cuatro países de América Latina sobre los que se hicieron los estudios que componen este libro (Brasil, Chile y México, Colombia) por una mezcla de razones prácticas y de representatividad de lo que sucede en la región. Las razones prácticas van desde la sede de Dejusticia, la organización que alojó el proyecto y que tiene su sede en Colombia, hasta la existencia de relaciones de cercanía y confianza con otras organizaciones de la región que trabajan temas sobre derechos digitales y protección de datos. En Brasil, tiene su sede Coding Rights, una organización que investiga temas relacionados con derechos humanos y el uso de tecnología desde una perspectiva feminista. En Chile, la organización Derechos Digitales, que desde hace más de 15 años estudia el tema. Y en México se encuentra la Red en Defensa de los Derechos Digitales (R3D), una organización experta en el uso de datos en la era digital.

Adicionalmente, consideramos que estos cuatro países son representativos para hacer una muy modesta radiografía del fenómeno en la región. Esta selección combina varios factores: su diferente ubicación geográfica, el tamaño de su población, adoptar como lenguas oficiales el español y el portugués, su relativo desarrollo normativo e institucional en la materia, y, por último, el tamaño de sus economías. Este último punto lo consideramos relevante porque funge como un incentivo para las EMNBD transnacionales que tienen presencia, o que buscan intensificarla, por fuera del domicilio de sus matrices.

Para resolver las preguntas que guían esta investigación y que mencionamos, readecuamos ligeramente la metodología utilizada en el trabajo previo de Newman y Ángel titulado *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital* publicado por Dejusticia en 2019. De tal forma que, en cada país, se identificaran cuatro EMNBD que correspondieran a las siguientes cuatro categorías: 1) grandes empresas de internet, que se destacan por

su amplio capital de inversión (GAFAM); 2) empresas intermedias, que se están consolidando pero no han alcanzado el nivel de las grandes empresas de internet; 3) *start-ups*, que se definen por su temprana edad y gran capacidad de crecimiento; y 4) empresas establecidas, que son comercios previos a la revolución digital que han ajustado su modelo de negocios a la era digital.

Una vez identificadas las EMNBD, se analizan las políticas de tratamiento de datos de sus productos más relevantes, con el fin de caracterizar su forma de operar de cara a los siguientes temas: 1) fuentes de datos, 2) tratamiento, 3) finalidades del tratamiento y 4) relación con GAFAM. A continuación, se evalúan 1) el nivel de preparación del régimen jurídico de protección de datos para abordar las dinámicas propias de la era digital, frente a las prácticas empresariales identificadas anteriormente y 2) las capacidades de la autoridad de protección de datos nacional —o, en su defecto, de los jueces— para hacer rendir cuentas a las EMNBD, teniendo en cuenta sus funciones de vigilancia, control y/o sanción. Finalmente, frente a los hallazgos y a los análisis del caso, se formularían recomendaciones.

El proceso de escritura de los resultados de la investigación contó, además, con la realización de un grupo focal en cada país (Brasil, Chile y México) con expertos en protección de datos, defensores de derechos humanos, miembros de la academia y representantes de la industria.

Una vez recibidos los informes por país, se adelantó un trabajo de comparación entre ellos, con el fin de que fungiera como una suerte de informe compilado regional. En este trabajo de comparación, integrado como el capítulo final del libro, se hace una descripción muy general de los principales hallazgos de los cuatro países, en los puntos ya descritos en la metodología que guía la elaboración de informes por país, y se busca poner el énfasis en los patrones o elementos comunes que son los que orientan las recomendaciones finales.

Finalmente, el trabajo de compilación, que incluye esta introducción, los informes por país y el estudio de comparación, fue sometido al escrutinio y comentarios de los autores de los informes por país, distintos actores del sector y expertos en la materia, en un grupo focal realizado el 20 de febrero de 2020, en la sede de Dejusticia en Bogotá, Colombia.

6. Informes por países

Siguiendo la metodología ya descrita, en el primer capítulo, Kimberly Anastácio, Bruna Martins dos Santos y Joana Varon analizan el ordenamiento jurídico brasileño (haciendo énfasis en la recientemente promulgada Ley 13.709 de 2018) a la luz de las prácticas de uso de datos personales de cuatro EMNBD que operan en Brasil: Amazon, iFood, Social Miner y Magazine Luiza.

Por su parte, en el segundo capítulo, Paloma Herrera y Pablo Viollier analizan en Chile la forma de operar de Facebook, PedidosYa, aira y Falabella. Su texto, además, contrasta los postulados de la Ley Nº 19.628 sobre protección de la vida privada, con el proyecto de ley que "Regula la protección y tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" que para la fecha de edición de este texto (febrero de 2020) se encontraba en discusión en el Congreso Nacional de Chile.

Posteriormente, en el tercer capítulo, María Paula Ángel, Vivian Newman y Daniel Ospina-Celis nos ofrecen un resumen de su investigación actualizada, pero previamente publicada bajo el título *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*. Este capítulo, a diferencia de los correspondientes a Brasil, Chile y México, analiza los términos de servicio de treinta EMNBD que operan en Colombia, junto con las disposiciones de la Ley 1581 de 2012 y las capacidades para hacer rendir cuentas a las EMNBD de su autoridad de protección de datos.

El quinto capítulo corresponde al análisis que hace Milan Trnka Osorio del régimen de protección de datos de México y del rol del Instituto Nacional de Transparencia y Acceso a la Información Pública (INAI) como autoridad de protección de datos. Este texto toma como punto de partida las políticas de privacidad de Amazon, Snap Inc. (dueña de Snapchat), Playclip S. de R.L. de C.V. y Radio Móvil Dipsa S.A. de C.V (propietaria de Telcel).

Por último, el sexto capítulo es un análisis de Daniel Ospina-Celis y Juan Carlos Upegui Mejía, en el que, a partir de los estudios por país referidos, hacen una comparación de los regímenes jurídicos y las prácticas comerciales de las empresas escogidas de Brasil, Chile, Colombia y México. Dicho capítulo pretende trazar puntos de encuentro entre los resultados de investigación de cada país, con el fin de determinar cuáles

son los desafíos comunes —en cuanto a las prácticas empresariales— y las necesidades compartidas de regulación —en cuanto al alcance de la legislación nacional o las capacidades de la autoridad de protección de datos—.

7. Alcance de la investigación

Debido a la metodología descrita anteriormente, y a la selección de apenas cuatro países de América Latina como objeto de estudio, la presente investigación tiene un alcance limitado. El análisis de la forma en que las EMNBD recolectan y analizan datos personales se basó principalmente en la lectura atenta de las políticas de privacidad de sus productos. No en un estudio técnico de las tecnologías de recolección y análisis usadas por cada empresa. Tampoco en un estudio empírico que incorporara metodologías cualitativas o cuantitativas para la recolecta y el análisis de la información. Lo anterior supone que, de existir diferencias entre lo reconocido por las empresas en su política de privacidad y su actuar efectivo, esto último quede por fuera del alcance de esta investigación. Adicionalmente, el limitado alcance del presente libro se agrava por la falta de transparencia y de exhaustividad en las políticas de privacidad analizadas.

Por otra parte, si bien las EMNBD analizadas en cada uno de los países pertenecen a un amplio espectro de compañías —debido a su tamaño y poder económico variado—, distan de ser una muestra estadísticamente representativa de todas las empresas con modelos de negocios basados en datos que operan en cada territorio. Este estudio no pretende ser estadísticamente significativo. Las empresas seleccionadas, más bien, dan cuenta de que es probable que las prácticas de tratamiento de datos personales sean similares (con algunos matices) entre distintas compañías en el marco de la economía digital. Lo anterior también aplica para los cuatro países seleccionados. No por ser un número representativo de países de América Latina los hallazgos aquí descritos nos permiten afirmar que los resultados de la investigación se pueden generalizar, sin matices, para los demás países de la región.

Daniel Ospina-Celis
Juan Carlos Upegui Mejía