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

Este texto puede ser descargado gratuitamente en http://www.dejusticia.org
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

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

Referencias

Barocas, Solon y Andrew Selbst. "Big Data's Disparate Impact". *California Law Review 104* (2016): 671-732.

Beduschi, Ana. Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society* (2019): 1-6.

Comisión Europea. *Germany: Industrie 4.0*. Digital Transformation Monitor. January 2017. Consultado octubre 15, 2019. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf

Corte Constitucional. Auto 285 de 2018, M. P. José Fernando Reyes Cuartas.

Corte Constitucional. Sentencia SU-420 de 2019, M. P. José Fernando Reyes Cuartas.

Corte Constitucional. Sentencia T-063A de 2017, M. P. Jorge Iván Palacio Palacio.

Culik, Nicolai. "Brussels Calling: Big Data and Privacy." In *Big Data in Context: Legal Social and Technological Insights* edited by Thomas Hoeren and Barbara Kolany-Raiser, 29-35. New York: Springer International Publishing, 2018.

De Mauro, Andrea, Marco Greco y Michele Grimaldi. *What is Big Data? A Consensual Definition and a Review of Key Research Topics.* Paper presentado en la 4ta Conferencia Internacional sobre Información Integrada, 2014.

Elgendy, Nada y Amed Elragal. Big Data Analytics: A Literature Review Paper. Lecture Notes in Computer Science, (2014): 214-227. Consultado diciembre 20, 2019. doi:10.1007/978-3-319-08976-8_16

Fondo Monetario Internacional. *Perspectivas económicas: Las Américas*. Washington: International Monetary Fund, 2019.

Grupo de Trabajo del Artículo 29. *Opinión 03/2013 sobre la limitación de finalidad*. Adoptada el 2 de abril de 2013, 00569/13/EN WP 203, 45. Consultado diciembre 20, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-ecommendation/files/2013/wp203_en.pdf

GSMA. (2018). *La Economía Móvil en América Latina y el Caribe 2018*. GSMA Association. Consultado octubre 16, 2019. https://www.gsmaintelligence.com/research/?file=6823ce60a8b9e547cb4ed1d85c6215d8&download

Hartmann, Philipp Max, Mohamed Zaki, Niels Feldmann y Andy Neely. *Big Data* for Big Business? *Cambridge Service Alliance Blog*. Cambridge: Cambridge Service Alliance, 2014.

Haupt, Michael. "Data is the New Oil" - A Ludicrous Proposition. *Medium*, 2016. Consultado octubre 16, 2019. Recuperado de: https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294

Kleinberg, Jon, Jens Ludwig, Sendhil Mullainathan y Cass R Sunstein. "Discrimination in the Age of Algorithms". *Journal of Legal Analysis* 10 (2018): 113-174.

Lu, Yang. "Industry 4.0: A survey on technologies, applications and open research issues". *Journal of Industrial Information Integration* 6 (2017): 1-10.

Newman Pont, Vivian, María Paula Ángel Arango. *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos en la era digital*. Bogotá: Dejusticia, 2019.

Organización de los Estados Americanos. Comité Jurídico Interamericano. *Privacidad y Datos Personales*, marzo 26, 2015. Consultado febrero 24, 2020. http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf

Pence, Harry. What is Big Data and Why is it Important? *Journal of Educational Technology Systems*, 43(2), (2014): 159-171. Consultado octubre 16, 2019. doi: 10.2190/et.43.2.d

Red Iberoamericana de Protección de Datos. *Estándares de protección de datos personales para los Estados iberoamericanos*, 20 de junio de 2017. Consultado febrero 24, 2020. https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ce (Reglamento general de protección de datos) 27 de abril de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

The Boston Consulting Group. *Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries*. The Boston Consulting Group, 2015. Consultado octubre 17, 2019. https://www.zvw.de/media.media.72e472fb-1698-4a15-8858-344351c8902f.original.pdf

Tribunal de Justicia. Sentencia C-505/17. Procedimiento prejudicial–Datos personales–Protección de las personas físicas en lo que respecta al tratamiento de estos datos–Directiva 95/46/CE–Reglamento (UE) 2016/679–Motores de búsqueda en Internet–Tratamiento de los datos que figuran en páginas web–Alcance territorial del derecho a la retirada de enlaces. Unión Europea: CVRIA. 24 de septiembre de 2019. Consultado mes día, año. http://curia.europa.eu/juris/document/document.jsf?text&docid=218105&pageIndex=0&doclang=ES&mode=req&dir&occ=first&part=1&cid=166644

Todorov, Tzvetan. *Los enemigos íntimos de la democracia.* Barcelona: Galaxia Gutenberg, 2012.

Vaidya, Saurabh, Prashant M. Ambad y Santosh P. Bhosle. "Industry 4.0–A Glimpse". *Procedia Manufacturing*, 2018.

Zuiderveen Borgesius, Frederik. *Discrimination, artificial intelligence, and algorithmic decision-making.* Consejo de Europa, 2018. Consultado enero 15, 2020. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

APLICACIÓN DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN BRASIL. ESTUDIO DE CASO DE ALGUNAS EMPRESAS CON MODELO DE NEGOCIO BASADO EN DATOS

*Kimberly Anastácio**
*Bruna Martins dos Santos***
*Joana Varon****

Introducción

La presente investigación fue realizada por Coding Rights en asocio con el Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia), como coordinadora de una investigación comparada entre Colombia, Chile, México y Brasil sobre la implementación de sus respectivas Leyes de protección de datos personales. Coding Rights, en calidad de institución asociada para realizar el estudio en Brasil, analizó las políticas de privacidad y los términos de uso de aplicaciones de servicios *online* que atienden al territorio brasileño para averiguar cómo se encuadran ellas en las disposiciones de la ley brasileña sobre protección de datos

* Licenciada y Magíster en Ciencia Política, Universidad de Brasilia. Fue investigadora en el Departamento de Políticas Públicas, Fundação Getulio Vargas y es coordinadora de datos, Isobar. Colabora con Coding Rights en temas de derechos humanos e internet.

** Abogada, Centro Universitário de Brasilia y analista de Coding Rights. Co-coordinadora de Internet Governance Caucus y miembro de Non-Commercial Users Constituency en la Corporação da Internet para Atribuição de Nomes e Números.

*** Directora ejecutiva de Coding Rights, fellow de Mozilla Foundation, afiliada al Berkman Klein Center for Internet and Society de la Universidad de Harvard, miembro del Consejo Consultivo de Open Technology Fund.

personales. Siguiendo la metodología del análisis comparado definida para el estudio, se seleccionaron cuatro empresas con modelos de negocio basados en datos (llamadas EMNBD). Así, para el grupo de grandes empresas de internet, se seleccionó a Amazon Prime Video; en el grupo de empresas intermedias, iFood; en la categoría *start-up*, Social Miner; y para la categoría de empresas establecidas, Magazine Luiza.

El artículo se divide en cuatro partes. En la primera, se exponen los criterios de selección de las cuatro empresas analizadas y se identifican cuatro aspectos principales en los términos de uso y políticas de privacidad de estas empresas: 1) la fuente de los datos recolectados, 2) el tratamiento de los datos, 3) la finalidad de su uso y 4) la relación de las empresas y de los datos recolectados con las empresas del grupo GAFAM. En la segunda, se analizan cómo las prácticas de estas empresas se ajustan al régimen jurídico de protección de datos en Brasil. Para ello, se observan las prácticas de las empresas seleccionadas para detallar los puntos que puedan ser contrastados con lo que dice la Ley de Protección de los Datos Personales (LGDP) y otros dispositivos referentes a la protección de los datos y de la privacidad, tales como el Código de Defensa del Consumidor, el Marco Civil de la Internet y la propia Constitución Federal. En la tercera parte, se evalúa si lo que hoy está previsto como forma de funcionamiento de la Autoridad Nacional de Protección de Datos Personales (ANDP), entidad responsable de la supervisión de la aplicación de la ley brasileña, efectivamente responde a las prácticas de las empresas mencionadas, principalmente en lo que respecta a su capacidad de regulación, supervisión, control y sanción. Finalmente, se presentan las conclusiones y recomendaciones para que la forma de operar de las EMNBD se ajuste cada vez más a los principios y a la regulación de la protección de datos personales en el país, sobre todo teniendo en cuenta la necesidad de que las empresas estén alineadas con la ley recién aprobada (LGDP) que entra en vigencia en el 2020.

1. Selección de las EMNBD

1.1. Empresa GAFAM: Amazon Prime Video

En este estudio se analiza tanto el servicio de video por demanda de Amazon Prime Video, como las especificidades de su oferta ligada a Vivo, concesionaria de telefonía brasileña integrante del grupo Telefónica. Desde septiembre de 2018, la operadora de telefonía Vivo, de la empresa

Telefónica, en asocio con Amazon comenzó a proporcionar el servicio de video *streaming* de Amazon Prime Video. Amazon Prime llegó en Brasil efectivamente en septiembre de 2019, cuando el presente estudio ya estaba en ejecución. Antes, desde septiembre de 2018, la operadora de telefonía Vivo, de la empresa Telefónica, tenía una asociación con Amazon para proporcionar el servicio de video streaming de Amazon Prime Video a sus clientes. Por lo tanto, analizamos en el estudio los documentos y políticas vigentes antes de septiembre de 2019, cuando aún el servicio era conjunto con Vivo. En este caso, la empresa ofrece 90 días de acceso gratuito, después cobra 7.90 reales durante los primeros seis meses y, al siguiente mes, comienza a cobrar 14.90 reales mensuales[1]. Pero, para suscribirse es necesario ser cliente Vivo del plan de celular o de la banda ancha. Amazon también ofrece directamente el plan en Brasil, pero solo da 7 días gratis, después el plan también tiene un costo de 7.90 reales por mes durante los primeros seis meses, y después pasa a valer 14.90 reales mensuales[2].

Además de que se considera que esta sociedad con Vivo es interesante en lo que respecta a la protección de datos, también es importante analizar a Amazon Prime Video en función de la disputa entre Google y Amazon en relación con el servicio, pues, después de varios meses de retaliaciones, los dos gigantes llegaron a un acuerdo y desde junio de 2019 el servicio está disponible para el ChromeCast (Gartenberg 2019).

1.2. Empresa intermediaria: iFood

Es una empresa de capital cerrado, fundada en 2011, y que hoy está presente en más de 200 ciudades (iFood s.a.) del país y en México, Colombia y Argentina. iFood es una plataforma de delivery de comida. El servicio, ofrecido en una versión web y en aplicaciones para iOS, Android y Windows Phone, cuenta con casi 600 mil pedidos por día en Brasil por parte de sus 12 millones de usuarios activos (Daroit 2019). La Empresa además posee un producto llamado iFoodLabs, un laboratorio de innovación enfocado en aplicar la visión de negocio a ideas que unen

---

1 Costos vigentes en la fecha de consulta disponibles en la p{agina web de Amazon Prime Video https://www.vivoparasuacasa.com.br/amazonprimevideo/?gclid=EAIaIQobChMIlba8weX_4wIVIlaRCh3epwrjEAAYASAAEgKRIvD_BwE

2 Costos disponibles a la fecha de consulta en la p{agina web de Amazon Prime Video https://www.primevideo.com/

tecnología y alimentación. Por medio de datos de mercado, experiencias, casos de uso de los clientes, entrevistas con *stakeholders* y especialistas, la idea del laboratorio consiste en utilizar metodologías de diseño para crear soluciones para el mercado de delivery de la cadena productora de alimentos. El laboratorio generó productos como el SpoonRocket[3] e iFoodNext, división concentrada en desarrollar software y servicios focalizados en las demandas de los dueños de restaurantes. La empresa también posee una plataforma llamada iFood Shop (Belloni 2018), que conecta los restaurantes con los proveedores de empaques e insumos.

La *start-up* ha recibido aportes de empresas como Móvile, que invirtió 5.5 millones de reales en 2013 (Zuini 2013) y 125 millones de reales (conjuntamente con la empresa británica Just Eat) en 2015. En noviembre de 2018, Móvile anunció que iFood recibiría una inversión de 500 millones de dólares (Brigatto 2018) que era el equivalente a 1.9 billones de reales —lo que representó el mayor aporte privado en una empresa privada de tecnología en Brasil—. La idea del aporte fue ampliar la actuación de iFood en el país y duplicar los números de restaurantes (actualmente cerca de 66 mil) y de las ciudades atendidas (500 municipios) (Freitas 2019). iFood ocupa el lugar 23 entre las aplicaciones más descargadas de la Play Store. La aplicación cuenta con más de 10 millones de descargas, es la más descargada de toda la Play Store en la categoría 'Comer y beber'.

1.3. Start-up: Social Miner

La empresa figura en varias listas de *start-ups* que merecen ser tenidas en cuenta en el país, al llamar la atención de programas de aceleración de *start-ups* liderados por empresas como Oracle (Social Miner 2018) y Google (Freitas 2019). La empresa no cuenta con una aplicación, sin embargo, desarrolló su propia plataforma de direccionamiento de propaganda *online*. Creada en 2014, declara tener el objetivo de "aproximar marcas y personas a la tecnología y mejorar los respectivos desempeños *online* por medio de la utilización de tecnologías de Inteligencia Artificial y Big Data" (Social Miner s.a.). La empresa identifica prácticas de consumo, perfiles de consumidores y metodologías de compromiso *online* con las marcas, por medio de una base de datos capaz de identificar una

3 Disponible en la página web de la aplicación (https://www.spoonrocket.com.br/)

"etapa de la jornada en que está un consumidor y su intención de compra" (Social Miner s.a. a) para que las empresas logren realizar propaganda direccionada/compromiso con aquellos consumidores que eventualmente no compran sus productos.

Social Miner es una empresa cuyos productos no tienen interacción con los usuarios finales, pues ofrece estrategias de compromiso y *marketing* digital para empresas, o para las contratantes. De acuerdo con el propio sitio web de la empresa, Social Miner ofrece una plataforma que les permite a las empresas contratantes —entre ellas Avon, Asus, Sephora Brasil, Natura, Extra y Wine.com.br (Social Miner s.a. b)—una mejor comprensión de los contextos y de los lenguajes ideales para incentivar a los consumidores indecisos, segmentar sus datos y crear campañas personalizadas.

1.4. Empresa establecida: Magazine Luiza

Magazine Luiza es una empresa especializada en el sector de ventas al por menor, cuya estrategia digital llamó la atención por poseer productos como una *bot*, Lu, con un canal en Youtube; por contar con programas que incentivan la producción del contenido de sus almacenes para Facebook, porque su aplicación cuenta con más de 10 millones de instalaciones en la Play Store Brasil (Google Play Store s.a.) y por ocupar el segundo lugar en las aplicaciones de compras más descargadas en el App Store Brasil (App Store s.a.).

Fundada en 1957 en Franca, São Paulo, la marca posee más de 900 tiendas físicas y 12 de distribución, extendidas por 17 estados brasileños (Magazine Luiza s.a.). Y ofrece productos de los sectores de muebles, electrodomésticos, electrónicos, regalos, juguetes, *hobby* y entretención, informática y telefonía, tanto en los almacenes físicos como en el sitio web y en la aplicación. Magazine Luiza introdujo el concepto de las tiendas virtuales en 1991, cuando sus tiendas no tenían productos físicos (Gazzoni, Cruz 2011). En esa época, las ventas se realizaban mediante terminales electrónicos y la entrega del producto se hacía hasta 48 horas después de la adquisición; la marca continúa usando el modelo de tienda virtual, lo que permite la existencia de tiendas sin suministros físicos o muestrarios. En 2013, la compañía introdujo sus asistentes electrónicas de ventas, Lu, creada para instruir a los usuarios sobre el uso de productos conectados, sobre cómo mejorar la navegación por el sitio web (Calado 2018) y, así, contribuir a la inclusión digital de los clientes (Fraga 2018).

Esta *avatar* digital ayudó al aumento de las ventas online en un 56 % en el primer semestre de 2017 (Bloomberg 2017), e incluso cuenta con un canal de Youtube[4] con 1.6 millones de seguidores.

La empresa tiene estrategias que son representativas para el desarrollo de su plataforma digital —además de las aplicaciones que ya se mencionaron: sitio web, tiendas virtuales, canal en Youtube y *avatar*— Magazine Luiza también fue pionera en la operación de ventas al por menor mediante el *Omni-channel* de Brasil (Ricciardi 2016). La operación de *Omni-channel* permite que varios canales de venta usen la misma infraestructura (centros de distribución, contabilidad, *marketing*). Algunas estrategias digitales de la compañía requieren atención, como el Programa Maga Local, el Marketplace e, inclusive, la acción de *marketing* en Tinder que les concedía descuentos especiales a los usuarios de la aplicación que le dieran *match* al perfil de Lu (Bloomberg 2017). Sobre el Maga Local y el Marketplace de la empresa, vale la pena destacar que el primero busca incentivar que las tiendas tengan *fanpages* propias en Facebook, y también autonomía para producir contenido; en cuanto al Marketplace de la empresa, lanzado en 2016, hoy permite que se ofrezcan en la aplicación y en el sitio web de Magazine Luiza productos de más de 500 empresas y representa un cuarto de las ventas digitales (Magazine Luiza 2019).

En un artículo de octubre de 2017, el presidente de Magazine Luiza, Frederico Trajano, señaló que la empresa pretendía enfrentar la expansión de la operación brasileña de Amazon con posibles refuerzos en los puntos físicos y con la integración de la tienda *online* con la tienda física. En ese momento, el comercio electrónico representaba el 30 % de los ingresos de Magazine Luiza, aproximadamente 4 billones de reales, y la aplicación ya contaba con 7 millones de accesos mensuales (Manzoni 2017).

2. Caracterización de la forma de operar de las EMNBD

2.1. Fuente de datos

Las ofertas de empleo en Amazon Prime Video revelan cómo la empresa pretende "moldear el futuro del entretenimiento en video". Por ejemplo,

4 Canal da Lu - Magalu. (https://www.youtube.com/user/magazineluizacom)

por medio de la contratación de personas para cargos como *Business Intelligence Engineers*, buscan "descubrir cómo los consumidores ven videos en Amazon" y "trabajar en una de las bases de datos más grandes de consumidores del mundo" (LinkedIn s.a.). Otro cargo ofrecido es el de líder del equipo de ingenieros y científicos de datos encargado de "definir y entregar mediciones de comportamiento y marketing de clientes" (Higa 2019). No hay duda de que la recolección y el tratamiento de datos personales de sus consumidores están en el centro del negocio.

En Brasil, lo que nos llamó la atención fue que esos servicios también son ofertados en asocio con Vivo, la empresa de telefonía móvil que, así como varias otras, ya fue investigada (Luna 2018) por sospecha de uso de datos personales.

Según el sitio web de Vivo, quien haya sido consumidor de sus planes de telefonía celular solo requiere enviar un SMS con la palabra Amazon para contratar Amazon Prime Video. La plataforma incluso está haciendo sociedades para la producción de contenido brasileño (Meio & Mensagem 2018). Entonces, el consumidor de ese servicio queda sujeto tanto a los términos de uso de Vivo (Vivo s.a.) como a los de Amazon Prime Video (Amazon 2019), en caso de presentarse un conflicto, Vivo declara que prevalecen sus términos.

Las fuentes de datos vienen tanto de lo dispuesto por el Centro de Privacidad de Vivo (Vivo s.a. a), como de los Términos de Uso (Amazon 2019) y el Aviso de Privacidad (Amazon 2017) de Amazon.

En los términos de uso de Amazon Prime Video, vinculados al contrato de suscripción al servicio con Vivo, o al buscar directamente en Amazon, cuando se quiere contratar el servicio directamente con la empresa extranjera, se encuentra información de que Video Marketplace de Amazon tiene diferentes proveedores y, por consiguiente, distintos términos y políticas aplicables que varían de región a región. Entre los países de América Latina, solo México aparece listado explícitamente. Los consumidores brasileños quedan encasillados en la categoría "Estados Unidos y todos los otros países no indicados arriba", cuyo proveedor es la sede de Amazon en Seattle. Los términos aplicables y las notificaciones legales son las siguientes, algunos disponibles solo en inglés:

- Amazon Prime Video Terms of Use (disponible en PT)
- Amazon Prime Video Usage Rules (disponible en PT)
- Condition of Use (solo disponible en ING)

- Privacy Notice (solo disponible en ING)
- Interest-Based Ads Policy (solo disponible en ING)
- Twitch Terms of Service (solo disponible en ING)

En los términos de uso de Amazon Prime Video, está dispuesto en la sección denominada 'Software' que "el servicio podrá suministrar a Amazon la información relacionada con su uso y desempeño, así como la información referente a los dispositivos que utilizan el servicio y el software" (Vivo s.a.). Allí se incluye la información sobre la manera en que se consume el contenido digital de la plataforma.

Los documentos de términos de uso y reglas de uso de Amazon Prime Video no disponen nada adicional sobre la protección de datos personales, pero afirman que esa información está sujeta al Aviso de Privacidad de Amazon que, a su vez, está disponible solo en inglés, incluso para quien contrata el servicio en Brasil.

En esos documentos se destaca que Amazon determina que puede recolectar los siguientes tipos de datos e información: 1) información que compartimos sobre nosotros mismos; 2) "información automatizada", donde se menciona el uso de *cookies*; 3) información sobre nuestros dispositivos, inclusive la confirmación de la recepción/lectura de emails de comunicación que envía a sus clientes; y, finalmente, 4) "información de otras fuentes", incluyendo la que va desde la dirección de entrega, datos de compras, visualización de páginas, resultado de búsquedas o términos utilizados en las búsquedas hechas por medio de Alexa e incluso información del historial de crédito de oficinas de crédito.

El Centro de Privacidad de Vivo describe la recolección de información sobre: 1) nuestros datos de registro como el nombre, la dirección, el CPF y otros informados en el contrato; 2) volumen de datos traficados en la internet; 3) historial de uso de los productos y de los servicios contratados, lo que, según la empresa, no involucra registros de aplicaciones que no sean de Vivo, ni de actividades en las redes sociales; 4) historial de llamadas y de SMS recibidos; 5) información contable y fiscal y datos de atención al cliente.

Por su parte, en el caso de iFood, según la política de privacidad, los datos recolectados y tratados por la empresa se concentran en tres fuentes principales. La primera son los datos proporcionados por el propio usuario/cliente. Al registrarse, el usuario se compromete a proporcionar información como el nombre, la dirección, el CPF, el correo electrónico,

el teléfono y la fecha de nacimiento. Con el uso continuo de la aplicación o del sitio web, la empresa recoge datos sobre el comportamiento del usuario en la plataforma, trazando un historial de sus compras y de su actividad dentro de la aplicación. Además, está la recolección de información sobre los datos de pago, con el número de las tarjetas de crédito de los clientes. Una parte vital para el funcionamiento de la aplicación es la recolección de datos de la ubicación, que pueden ser suministrados por el usuario o recolectados por el GPS y las redes móviles del celular registrado. Según la política de privacidad, tal información es "para fines de la Ley N° 12.965 de 2014 (Marco Civil de la Internet), o de cualquier ley que la sustituya, [...] será considerada como dato de registro".

La segunda fuente son los datos compartidos por los socios estratégicos. En ese caso, existe la posibilidad de que el cliente haga su *login* directamente con la cuenta de Facebook, permitiendo que iFood recoja los datos de esa red asociados directamente a la identidad del cliente, como el nombre, el género, la edad. La tercera fuente de datos proviene de webtracking. Según la política de privacidad, iFood puede recolectar información automáticamente de los dispositivos usados para el uso de la aplicación, incluyendo "direcciones IP, tipo de navegador e idioma, proveedor de servicios de internet (ISP), páginas de consulta y salida, sistema operacional, información sobre fecha y horario, datos sobre la secuencia de clicks, fabricante del dispositivo, operadora, modelo, redes Wi-Fi, número de teléfono".

La política de privacidad de iFood también declara que la información sobre las actividades de los usuarios en la Web o en la aplicación será considerada como datos agregados e información no personal. La política de privacidad también dispone que "la edad del individuo, las preferencias individuales, el idioma, el CEP y el código de área" son considerados datos no personales, mientras que no se combinen con los datos personales del individuo en cuestión.

En cuanto a Social Miner, en un artículo publicado en el sitio web "Proyecto Draft" (Souza 2016), la empresa fue citada como una iniciativa promisoria que "usa inteligencia artificial, perfil social y comunicación para automatizar las campañas de marketing digital con un alto grado de personalización". Social Mine alega que introdujo el factor humano en las tecnologías ya desarrolladas para el marketing digital, con el concepto de que estas definen el *"people marketing"* —o la entrega al usuario de un direccionamiento hecho exclusivamente para él—.

De acuerdo con el mismo artículo, el compromiso de Social Miners se da de la siguiente forma:

> Imagínese que usted está navegando en un e-commerce que contrata Social Miner y que resuelve salirse del sitio web. Al notar el movimiento del cursor del ratón hacia afuera de la pantalla, el algoritmo percibe que usted no irá a realizar la compra en ese momento y le ofrece un beneficio para que permanezca en contacto con la marca, que puede ser un cupón o incluso el acceso a sugerencias exclusivas. También puede ser un pop-up (que no impide que usted cierre la página).
>
> Cuando el usuario decide hacer el login a través de Facebook, la plataforma obtiene los datos que vuelven posible llamarlo por el nombre y direccionar el contenido según su ciudad, sexo y franja etaria, por ejemplo. A partir del momento del registro, el algoritmo de Social Miner comienza a monitorear el perfil de navegación en el sitio web para entender el comportamiento del usuario: qué productos vio, si ya hizo alguna compra en la tienda, etc.
>
> Después de recolectar esa información, es la hora de hablar con el usuario, en el momento correcto (Souza 2016).

Frente a lo dispuesto arriba, queda claro que la plataforma de direccionamiento de contenido que ofrece Social Miner es alimentada por los datos de navegación de los usuarios, además de los datos de *login* en plataformas como Facebook. Es importante mencionar que, con los datos recolectados y los servicios ofrecidos, la *start-up* publicó el informe llamado "O comportamento do consumidor Online em 2018" (Social Miner 2018) que contiene el análisis del perfil de consumo de 35 millones de personas registradas en su base de datos, así como las estadísticas de desempeño en sitios webs de *e-commerce*.

El '*people marketing*' —concepto desarrollado por Social Miner— ha llamado la atención de los programas de aceleración de *start-ups* liderados por empresas como Oracle y Google. La empresa, con 5 años de existencia, también cuenta con la inversión de fondos como Canary, Wayra (Grupo Telefónica) e Indicador Capital.

La empresa afirma que actúa en concordancia con el reglamento europeo, además de velar por la seguridad de los datos y la privacidad de los usuarios (Social Miner s.a. c). Por eso, la herramienta enumera una

serie de ocho derechos de los usuarios afectados por la empresa (Social Miner s.a. c). Esa lista incluye, entre otros, el derecho de ser informado sobre cualquier dato recolectado y de exigir ajustes en la recolección, el derecho de prohibir la recolección de nuevos datos y el derecho de "contestar decisiones hechas por medios automatizados, o la elaboración de perfiles, si tales decisiones llegaran a tener el poder de producir efectos jurídicos para sí mismo, u otro efecto igualmente significativo" (Social Miner s.a. c).

En relación con la recolección de datos, para el contrato proactivo del equipo de ventas, Social Miner recoge información como nombre, correo electrónico, teléfono, sitio web de la empresa, sector o categoría de negocio y tráfico del sitio web de la empresa "siempre que un visitante descargue algún material educativo, realice un registro en nuestro sitio web o participe en algún webinar o evento organizado por Social Miner" (Social Miner s.a. c).

Además, siempre que un usuario navega en el sitio web de la empresa, la visita se transforma en un dato procesado por Google Analytics. En caso de que la conexión se haga mediante Facebook, o sea, en el caso de que el usuario cree un *login* por medio de Facebook, la información pública del perfil también se recoge. En el caso de que el usuario dé un 'aceptar' (opt-in) por medio de un click en las notificaciones del propio sitio web, se recolectan los datos del nombre, correo electrónico e información de Cookie" (Social Miner s.a. c).

En relación con el funcionamiento de la plataforma y la recolección de datos de los usuarios que navegan en los sitios web de los clientes de Social Miner, los datos recogidos son los mismos mencionados arriba cuando hay un opt-in de los usuarios. La herramienta está poderosamente amparada en la recolección y análisis de *cookies*. Por eso, posee un documento separado con la "política de *cookies*" (Social Miner s.a. d) de la empresa.

Tal política afirma que Social Miner recolecta *cookies* "persistentes", o sea, "todos aquellos que, independientemente de la navegación, siempre se mantienen registrados en el servidor de Social Miner" y de una "sesión", o sea, los "comportamientos de navegación dentro de una única ventana de navegación del usuario" (Social Miner s.a. d).

Para los fines de la empresa, *cookies* de una sesión se subdividen en:

- *Cookies* de análisis, que posibilitan el reconocimiento y el conteo del número de visitantes.

- *Cookies* de reconocimiento, que buscan reconocer la retroalimentación de los usuarios al sitio web o a la tecnología.
- *Cookies* de rastreo, que tienen como función el registro de la visita al sitio web o a la tecnología, cuáles páginas fueron frecuentadas y la información adicional de navegación.

Además, la política de privacidad (Social Miner s.a. c) afirma que:

> Cuando alguien se convierte en cliente de Social Miner, usamos plugins de conexión, en especial el Facebook Login, para crear una base de usuarios para la marca del cliente. Los avisos y pantallas de conexión podrán aparecer al final de la navegación de cada usuario o al inicio, cuando el mismo demuestra la intención de salir del sitio web del cliente, de tal forma que no perjudique la navegación o interfiera los eventuales procedimientos de compra.

Con respecto al Magazine Luiza, el documento relacionado con la política de privacidad de la empresa (Magazine Luiza 2015) comienza aclarando algunas definiciones iniciales, para los efectos del documento en referencia:

> *Cookies*: archivos enviados por el servidor del sitio web al computador del usuario, con la finalidad de identificar el computador y obtener los datos de acceso como páginas navegadas o links pinchados, permitiendo, de esta manera, personalizar el uso del sitio web, de acuerdo con su perfil.
>
> IP: abreviatura para Internet Protocol. Es un conjunto de números que identifica el computador del Usuario en la Internet.
>
> Logs: registros de las actividades del Usuario realizadas en el sitio web.
>
> Sesión ID: identificación de la sesión del Usuario en el proceso de inscripción o cuando el sitio web es utilizado de alguna forma.
>
> Usuario: todo aquel que use el sitio web.

Tanto el *e-commerce* de Magazine Luiza como la aplicación tienen la misma política de privacidad elaborada el 23 de julio de 2015. El documento dispone que la recolección de datos será realizada a partir del momento en que el usuario: "(a) comience a usar el sitio web; (b) interactúe con las diversas herramientas existentes en el sitio web, suministrando

la información voluntariamente; o (c) entre en contacto a través de los canales de comunicación disponibles en el sitio web (Magazine Luiza 2015)". En la acción de registro del sitio web y de la aplicación, el usuario además de tener la edad mínima de 18 años, debe suministrar los siguientes datos: nombre completo, apodo, CPF, RG, dirección completa, teléfono fijo, fecha de nacimiento, correo electrónico.

Sin embargo, una *hotpage* de la aplicación en el *google store* aclara que esta puede recoger datos como la ubicación aproximada del usuario (mediante la red) y la ubicación exacta del usuario (por medio del acceso al GPS). Además, la aplicación pide autorizaciones para realizar llamadas directamente, acceder a los datos de la SD card de los celulares de los usuarios y puntos como el uso de los datos para Installer API, acceso directo a la Internet, leer los servicios de configuración de Google, recibir datos de la Internet, y el acceso a conexiones de red y wi-fi.

Además de los datos dispuestos arriba, la política de privacidad de la empresa dispone que podrá recolectar datos referentes a la actividad de los usuarios en el sitio web, por medio de logs. Los logs en cuestión incluyen dirección de IP del usuario, acciones realizadas en el sitio web, páginas consultadas, fecha y hora de acceso a las funcionalidades del sitio web y a cuáles, sesión ID del usuario.

2.2. Tratamiento y finalidades

El Aviso de Privacidad de Amazon declara que la "información que recogen de sus clientes ayuda a personalizar y mejorar sus productos", y el documento sobre "Anuncios basados en el interés" (Interest-Based Ads) aborda la práctica de los anuncios direccionados. De acuerdo con la "Privacy Notice", la información es compartida con 1) los "negocios afiliados que Amazon no controla", 2) con "terceros proveedores de servicio" que realizan funciones subsidiarias al negocio de Amazon en nombre de la empresa (para enviar ofertas para grupos específicos, en ese caso, es posible el opt-out), 3) en caso de compra y venta de nuevas subsidiarias o unidades de negocios y 4) en caso de protección de Amazon.com y otros, por razón de sospecha de fraude u otra ilicitud. Finalmente, después de enumerar esas hipótesis de tratamiento y de las finalidades de compartir la información, el documento resalta que, en otras hipótesis en las que los datos pueden ser transferidos a terceros, sus consumidores son notificados para expresar o no su consentimiento.

En la Central de Privacidad de Vivo, se tiene acceso a los términos de Tratamiento de Datos Personales[5], de distinta manera a la mencionada en la Central de Privacidad, los términos no clasifican las fuentes de datos, ni menciona las formas de tratamiento, sino que dispone que la contratada, en este caso, la Telefónica, tiene la obligación de tratar los datos personales en la medida de lo necesario para la prestación del servicio, siendo vetado el tratamiento para otras finalidades, a no ser que exista una autorización expresa. Y, a renglón seguido, dispone sobre otras obligaciones, como la transparencia para tratar los datos de sus clientes.

En cuanto a la Central de Privacidad, esta ejemplifica las razones para recolectar la información de los clientes:

> (a) transacciones de recargas y uso de crédito; (b) mejorar el desempeño de la red y corregir fallas; (c) personalizar procesos de elaboración de planes; (d) evaluar la demanda por región; (e) ayudar en la toma de decisiones estratégicas de Vivo, con la redistribución de la señal o la reorganización de la cartera de servicio; (f) y marketing directo.

Cabe anotar, por lo tanto, que la información sobre un mismo asunto, el tratamiento de datos, se encuentra dispersa y es presentada de distinta manera en diferentes documentos o lugares de información. Así como tampoco queda muy claro en los ítems c y f si los datos personales son usados para la formación de perfiles.

Por su parte, iFood afirma en su política de privacidad que los datos recolectados son usados para mejorar sus productos y desarrollar otros nuevos, así como para promover auditorías, análisis estadísticos sobre el uso de los servicios, incluyendo tendencias de consumo y

> "servicios y comunicaciones con los clientes", sin detalles sobre lo que configurarían tales servicios. La empresa aún deja claro en su política que usará los datos de feedback de las compras, o sea, el recibo dado por cada usuario a cada compra en la aplicación para "publicar y usar tales comentarios y feedbacks en el sitio web o en la aplicación y en cualquier material de marketing o publicidad, así como para analizar, procesar y tratar ese feedback de forma aislada o agregada" (iFood 2018).

---

5 TELEFÔNICA, Termo de Tratamento de Dados Pessoais, julho, 01, 2019. https://www.vivo.com.br/portalweb/ShowPropertyServlet?nodeId=/ucmrepository/contrib_269712

Con este fin, la aplicación identifica al cliente y su feedback "a través de su nombre de registro, de la foto del perfil de iFood (en caso de existir) y de su ciudad de residencia (iFood 2018)".

Además de eso, dispone que los datos también son usados para "analizar y solucionar problemas técnicos, así como para identificar y evitar fraudes en el uso del [...] Servicio" (iFood 2018) y para el envío de notificaciones y de comunicados importantes, como alteraciones en las políticas, alteraciones en los plazos, comunicados que no pueden ser desactivados por el cliente por ser considerados inherentes al servicio. Una sección específica de la política de privacidad muestra la posibilidad del uso de los datos con fines de marketing digital (direccionado en redes sociales y notificaciones *push*) y no digital (como radio, panfletos, outdoors).

Otra sección está dedicada a la explicación de la recolección de *cookies* y afines. Según la sección, "iFood utiliza tecnologías como *cookies*, *pixel tags*, almacenamiento local u otros identificadores, tanto de dispositivos móviles o no, o de tecnologías similares ("*cookies* y otras tecnologías"), para una variedad de funciones", como, por ejemplo, para "autenticar su cuenta, promover y perfeccionar los servicios de iFood, personalizar su experiencia y evaluar la eficiencia de nuestra comunicación y publicidad" (iFood 2018). Para iFood esta información es considerada como no personal, siempre y cuando no sea combinada con información personal.

Aún más, la política de la empresa les ofrece a los clientes ejemplos del uso de tales datos:

> Saber su primer nombre nos permite darle la bienvenida la próxima vez que usted ingrese a iFood. Conocer su país e idioma nos permite viabilizarle una experiencia de compras personalizada y más útil. Saber que usted adquirió determinado producto o usó un determinado servicio permite hacer que su publicidad y comunicación de e-mail sean más relevantes para sus intereses (iFood 2018).

En relación con los terceros, iFood afirma que podrá compartir los datos con los socios con el fin de desarrollar campañas de marketing más asertivas y que "solamente compartirá los datos con los socios que tengan una política de privacidad que ofrezca niveles compatibles de protección a lo ofrecido" (iFood 2018) por su política. Además, los terceros que

realicen marketing dentro de la aplicación o sitio web de iFood, o sea, que promuevan la propaganda de productos de terceros en tales espacios, "pueden usar *cookies* y otras tecnologías propias en los servicios de iFood, tales como: Facebook, Google Analytics e Double Click" (iFood 2018) para contrastar el funcionamiento de las campañas de marketing.

La política de privacidad afirma que los integrantes del grupo iFood también podrán acceder a algunos de los datos de los clientes, así como a las empresas de procesamiento de pagos, a las empresas asociadas que entregan los pedidos, los servicios de redes sociales (cuando el cliente comparte directamente en su Facebook una compra reciente, por ejemplo) y, en el caso de información como nombre y foto de perfil, con otros usuarios de la aplicación.

La empresa también afirma que el almacenamiento de los datos se da "en servicios de nube confiables de socios que pueden estar localizados en Brasil o en otros países que ofrecen servicio de almacenamiento de nube confiables y usualmente utilizados por empresas de tecnología" (iFood 2018) y retenidos por el tiempo determinado por la legislación aplicable.

Inclusive, la empresa se propone cumplir la legislación acerca de la transferencia de datos para las autoridades judiciales, pero va más allá, afirmando que "iFood se reserva el derecho de compartir información sobre sus usuarios con terceros cuando existan motivos suficientes para considerar que la actividad de un usuario es sospechosa, ilegal o perjudicial para iFood o para algún tercero" (iFood 2018).

En relación con la seguridad, iFood afirma que sigue "privacy by design". La empresa no detalla lo que sería tal indicativo, pero afirma en la misma sección que: "Solo tratamos sus datos mediante un alto grado de seguridad".

Por su parte, la política de privacidad de Social Miner define, en su apertura, que quien

> no esté de acuerdo con el contenido de esta política, recomendamos no bajar nuestros materiales, ni utilizar cualquiera de nuestros servicios y, en caso de que los haya bajado o utilizado y quiera ejercer sus derechos de restricción, rectificación, exclusión u oposición, entre en contacto a través de privacy@socialminer.com (iFood 2018).

Sobre el uso de los datos, la empresa afirma que los que son recolectados serán usados por el equipo de marketing para un contrato

proactivo del equipo de ventas. Además, la empresa afirma que podrá cruzar los datos recolectados por medio del *login* de Facebook con datos de navegación, "de tal forma que se permita una mayor personalización de los mensajes enviados por nuestra empresa" a los clientes (Social Miner s.a. c).

Los datos recolectados de usuarios en sitios webs de los clientes de Social Miner sirven, incluso, para "una mayor personalización de los mensajes enviados por la empresa (contratante), bien sea como un análisis del comportamiento de la compra hecho automáticamente por los algoritmos de la inteligencia artificial" de la empresa (Social Miner s.a. c). O sea, el cruce de los datos recolectados, sobre todo los *cookies* de navegación, que viabilizan la personalización de la propaganda recibida por los usuarios que ingresan a los sitios web de las empresas que contratan los servicios de Social Miner.

Así, los datos personales recolectados de los usuarios son usados y procesados de forma automatizada por los algoritmos para entender los patrones de comportamiento y para crear audiencias segmentadas para las campañas hechas por la plataforma. Según la política de privacidad, la empresa utiliza la "automatización en el procesamiento de datos para analizar los movimientos del usuario o de los visitantes dentro del sitio web, identificando los contenidos y los productos de interés y, con base en eso, sugerir productos de forma personalizada para las preferencias individuales" (Social Miner s.a. c).

Según la política, los datos "generales de registro y clics serán usados para optimizar las campañas hechas a través de nuestra plataforma y estarán siempre a disposición (de los contratantes), pudiendo ser extraídos en cualquier momento, o integrados al software del CRM (de los contratos)" (Social Miner s.a. c). CRM es la sigla para "Customer Relationship Management", herramienta que facilita la suscripción y el registro de la información de cada cliente. Los usuarios del sitio web del contratante, según el documento, tienen derecho de retirarse de la suscripción de la base de datos, aunque no haya claridad sobre cómo fue hecho tal pedido y cómo los usuarios toman conocimiento de tal posibilidad.

Además de eso, la política de privacidad afirma que los datos recolectados por la empresa también "serán usados solo para cobranzas eventuales de servicios, comunicados internos y envío de materiales educativos o para generar investigaciones de mercado". Sobre tales investigaciones, Social Miner define que "los datos usados para los estudios generales

del comportamiento del consumidor borrarán la información personal de los usuarios" y que, en ese caso, estos datos ya no son personales, y sí un "mero conjunto de datos anónimos con fines del estudio y de la investigación" (Social Miner s.a. c).

Sobre la protección de los datos recogidos, la empresa afirma que el acceso a los datos personales "está restringido a los funcionarios de Social Miner, más específicamente a las áreas de ventas, de finanzas y de marketing" y que ninguna información personal podrá ser divulgada públicamente. Además de eso, la empresa afirma que "se compromete a no vender, alquilar o traspasar su información a terceros" a no ser que sea exigida judicialmente (Social Miner s.a. c).

El acceso a los datos de los usuarios por parte del contratante se hace con base en el comportamiento de los usuarios y de la individualización de campañas, sin que el contratante consiga acceder al comportamiento individualizado de un usuario directamente en la plataforma de Social Miner. Además, la empresa afirma que está terminantemente en contra de la 'cookiepool', es decir, la práctica de compartir las bases de datos sobre *cookies* entre sus clientes, o sea, entre los sitios webs de las empresas contratantes.

Finalmente, se destaca que la política afirma que, "en caso de que usted sea un usuario visitante de un cliente de Social Miner, le recomendamos que entre en contacto directo con el cliente, ejerciendo sus derechos de privacidad" (Social Miner s.a. c). También afirma que no recoge datos de menores de 13 años. Sobre el periodo de almacenamiento, la empresa afirma que mantiene los datos mientras sea necesario para el suministro de los servicios, mientras posean el consentimiento para ello o cuando sea determinado por la ley, borrando ciertos datos inactivos después de un lapso de 5 años.

En relación con Magazine Luiza, la política de privacidad de la empresa aclara que los datos y la información recogidos serán agregados al banco de datos del sitio web de Magazine Luiza, de titularidad y de propiedad de la empresa. Los datos en cuestión serán almacenados en un ambiente seguro al que solo accederán las personas calificadas y autorizadas por la empresa. Sin embargo, la empresa se exime de eventuales daños y perjuicios ocasionados por fallas, virus o invasiones al banco de datos del sitio web, salvo en los casos de dolo o de culpabilidad de la empresa.

La empresa también aclara que los datos de los usuarios no serán compartidos, vendidos o presentados a terceros. Adicionalmente, dispone

que el usuario del sitio web y el titular de los datos está apto para agregar, excluir o modificar cualquier información ligada a su perfil.

En lo que atañe al tratamiento de los datos, la política de privacidad aclara que los datos personales recolectados podrán ser utilizados para los siguientes fines:

> 1) Efectuar cualquier comunicación resultante de una actividad del propio sitio web o la identificación del respectivo destinatario; 2) Responder a eventuales dudas e solicitudes del usuario; 3) Suministrar el acceso al área restringida del sitio web o a sus funcionalidades exclusivas; 4) Cumplir la orden legal o judicial; 5) Constituir, defender o ejercer regularmente los derechos en el ámbito judicial o administrativo; 6) Elaborar estadísticas generales, para la identificación del perfil de los usuarios y para desarrollar campañas Magazine Luiza; 7) Garantizar la seguridad de los usuarios; 8) Mantener actualizadas las suscripciones de los usuarios con fines del contacto autorizado para ser realizado por teléfono, correo electrónico, SMS, correo directo o por otros medios de comunicación; 9) Informar sobre las novedades, promociones y eventos de Magazine Luiza y sus socios comerciales (Social Miner s.a. c).

La empresa incluso se reserva el derecho de enviar correos electrónicos diarios con ofertas a los clientes suscritos, que podrán ser cancelados por medio de interrumpir la suscripción mediante un link presente en todos los correos promocionales.

Finalmente, en relación con las *cookies*, MagaLu aclara que puede utilizar el primero, y que el usuario los puede deshabilitar en su navegador de preferencia. Respecto de los datos del registro de actividades, la empresa se reserva su uso para verificar los casos de investigación de fraudes o de alteraciones indebidas en sus sistemas y suscripciones.

2.3. Relación con las empresas GAFAM

En cuanto a Amazon Prime Video, se observa una relación directa con la empresa Brasileña Vivo, lo que afecta la comprensión sobre dónde comienza y dónde termina la relación de esas dos empresas con los datos. La multiplicidad de documentos que tratan el tema, en las dos plataformas, vuelve inviable una comprensión informada, bien sea del consumidor común, o de los consumidores que tengan más afinidad con el debate de protección de datos.

Si se tiene en cuenta la conexión de iFood con las GAFAM, se perciben tres tipos de relaciones. En primer lugar, la empresa permite que los usuarios accedan a sus cuentas por medio de sus perfiles en Facebook. La otra opción es mediante la realización de una nueva suscripción con el correo electrónico personal, pero es menos destacada en la aplicación. En segundo lugar, al menos la política de privacidad declara la posibilidad de la existencia de botones de redes sociales, en los que los usuarios podrían compartir directamente en su Facebook los detalles de sus pedidos. En tercer lugar, iFood usa Google Analytics, recogiendo información sobre el comportamiento de los usuarios en el sitio web para mapear las tendencias.

De esta manera, iFood deja disponible la información para las GAFAM y recolecta los datos de estas. Por ejemplo, sobre Facebook, la política de privacidad afirma que:

> Al utilizar Facebook para inscribirse en nuestro servicio, usted estará permitiendo que iFood tenga acceso a la información personal de su cuenta de Facebook, como su nombre, e-mail, género, edad y teléfono (en el caso de que lo haya registrado en Facebook). La información que podremos obtener, en ese caso, depende de su configuración de la privacidad del servicio de la red social (Social Miner s.a. c).

Si se analiza la relación de la aplicación con iFood, se presentó un caso en 2018 de un rumor que circuló en las redes y que afectó algunos perfiles de Facebook. Algunos usuarios cambiaron su apellido en Facebook al de "iFood" para obtener un cupón de descuento en la aplicación. Sin embargo, dicho cupón era una mentira, y los usuarios que realizaron la alteración, debido a las políticas de la propia plataforma, se vieron obligados a mantener el cambio de nombre por un mínimo de 60 días[6].

También, existió una iniciativa de iFood de crear un bot que interactuaba con los usuarios a través de Facebook Messenger para que los usuarios pudieran realizar pedidos directamente de la red social. Dicha funcionalidad ya no está operando (Letieri 2019). Además, Google tiene la función de realizar compras en aplicaciones de los dueños de celulares

6 LETIERI, R. (2019). Usuários colocam iFood no sobrenome e não conseguem mudar. Techtudo. Disponible en: https://www.techtudo.com.br/noticias/2019/05/usuarios-colocam-ifood-como-sobrenome-no-facebook-e-nao-conseguem-mudar.ghtml

de forma más rápida. Bautizado como "Pagar con Google", ese recurso funciona para realizar compras en iFood y Magazine Luiza (Gazeta Do Povo, 2017).

Con respecto a la relación de Social Miner con las empresas que integran GAFAM, la empresa se reserva el derecho de cruzar los datos de navegación y el *login* de Facebook con fines de perfeccionar los productos ofrecidos. La plataforma de direccionamiento del contenido ofrecida por Social Miner se alimenta de los datos de navegación de los usuarios, además de los datos de *login* en plataformas como Facebook.

La política de privacidad de la empresa menciona que los datos de navegación de los visitantes al sitio web y a la plataforma serán transformados en datos por Google Analytics y que, en caso de que el visitante se conecte con la marca mediante el login de Facebook, se utilizará su información pública básica como nombre, edad, sexo, así como sus datos de navegación, para permitir una mayor personalización de los mensajes enviados por la empresa.

Otro punto relacionado con Facebook queda claro cuando el mismo documento menciona el uso de plugins de conexión, en especial el *login* de Facebook, para crear una base de usuarios/clientes para la marca contratante. Inclusive, la empresa ofrece la posibilidad de mostrar avisos y pantallas de conexión con la red social al inicio de la navegación o cuando el consumidor desee salirse del sitio web de una determinada marca. O sea, la eventual recolección de datos personales de los usuarios realizada por Social Miner para la creación de bases de datos puede no ser debidamente informada al consumidor.

Sobre MagaLu, la conexión clara del sitio web y la aplicación con las GAFAM se hace por medio de la autenticación con el Perfil de Facebook y la Cuenta de Google, aunque la aplicación aclara que ningún contenido será publicado en nombre de los titulares de las cuentas. Además de eso, ambas plataformas permiten que se compartan las ofertas por medio de Facebook, Twitter, Google Plus, Whatsapp y el email personal. La política de privacidad no dispone nada sobre el uso compartido de datos con las plataformas o sobre el uso de Google Analytics para analizar los comportamientos de compra de sus usuarios.

Sin embargo, la estrategia digital de la empresa tiene mucho involucramiento con Facebook. En 2012, MagaLu presentó la idea de habilitar las tiendas en la plataforma Facebook y de constituir una red

de *e-commerce* en donde los usuarios podrían constituir sus propias tiendas que estarían afiliadas al Magazine Luiza (Jesús 2012).

Otro programa interno de la empresa llamado *Magazine Você* tenía el objetivo de remunerar a los usuarios con pequeñas comisiones si recomendaban determinados productos en las redes sociales. De acuerdo con el website tecnoblog (Veloso 2012), el programa funcionaba de la siguiente manera:

> Al tener una cuenta en Facebook, los usuarios de la red social ya pueden usar la aplicación Magazine Você para recomendar productos ofrecidos por Magazine Luiza a sus amigos del servicio. La lógica de funcionamiento es similar a la de cualquier programa de afiliados: hay una comisión por ítem vendido, referido a un porcentaje calculado sobre el valor de la venta.

Al tener una cuenta en Facebook, los usuarios de la red social ya pueden usar la aplicación.

En el sitio web de la empresa ya no es posible encontrar información sobre Magazine Você y la página del programa en Facebook ya no se encuentra disponible.

3. Evaluación del régimen jurídico de protección de datos personales para abordar las dinámicas de las empresas analizadas

3.1. Régimen jurídico de protección de datos en Brasil

Desde 2018, Brasil cuenta con una Ley General de Protección de Datos Personales (Ley 13 709/2018), que ha sido objeto de intensas discusiones entre los *stakeholders* del país y de arreglos políticos. Sin embargo, incluso antes de su aprobación, Brasil ya contaba con legislaciones previas que salvaguardaban, en alguna medida, los derechos a la privacidad. La Constitución Federal, el Código de Defensa del Consumidor (Ley 8078/90), la Ley del Habeas Data (Ley 9507/97) y el Marco Civil de la Internet (Ley 12 965/2014) y el Decreto que lo reglamenta (Decreto 8.771/16) delimitaban los principios y las directrices para la protección de la privacidad (Privacy International 2019). Además de eso, varias regulaciones sectoriales (Monteiro 2017) también tratan, aunque tangencialmente, sobre la protección de los datos personales, principalmente en los sistemas financiero y de salud. Sin embargo, hasta la aprobación

de la LGDP, el Marco Civil de Internet, ley sancionada en 2014, fue la primera legislación que trató específicamente sobre la protección de datos en Internet.

Después de una serie de consultas multisectoriales, el Marco Civil de Internet se convirtió en una legislación conocida y reconocida internacionalmente y sirve, entre otras cosas, como una carta de derechos y deberes en la Internet en Brasil. También fue la fuente más directa de direccionamiento para lo que se consolidaría en la LGDP, en relación con la protección de los datos personales, la fundamentación del derecho a la privacidad y a la introducción de la noción del consentimiento de acuerdos en Internet.

Por ejemplo, tal ley presentó disposiciones iniciales importantes sobre la protección y lo atinente a compartir los datos de los usuarios. Los Artículos 10 y 11 afirman positivamente la importancia del cuidado en la recolección, el tratamiento y la transmisión de los datos de los usuarios de Internet. Por ejemplo, establecen que los proveedores de Internet solo pondrán a disposición los registros de conexión y de acceso de aplicaciones de Internet mediante una orden judicial. Específicamente, el Artículo 11 afirma que:

> En cualquier operación de recolección, almacenamiento, protección y tratamiento de registros, de datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de internet en que al menos uno de esos actos ocurra en el territorio nacional, deberán ser obligatoriamente respetados la legislación brasileña y los derechos a la privacidad, a la protección de los datos personales y al sigilo de las comunicaciones privadas y de los registros.

De forma aún más clara, la ley defiende "la inviolabilidad de la intimidad y de la vida privada, su protección e indemnización por el daño material o moral debido a su violación" durante el uso de la Internet (Artículo 7). Especialmente, el Marco Civil también lanzó las bases para lo que, salvo excepciones expresas, la LGDP consolidaría como unas de las medidas necesarias para la recolección de datos: esto es el consentimiento de los usuarios. El texto dice, en su Artículo 16, que:

> En la provisión de aplicaciones de internet, onerosa o gratuita, está prohibida la custodia: I – de los registros de acceso a otras aplicaciones de internet sin que el titular de los datos haya dado su consentimiento previamente [...] II – de datos personales

> que sean excesivos en relación con la finalidad para la cual fue dado el consentimiento por parte de su titular.

Por el hecho de solo tratar el caso de Internet, el Marco Civil no solucionó todas las áreas grises en relación con la protección de datos en el país, aunque, aun así, ya señalaba algunos principios y responsabilidades. A propósito, incluso antes de la aprobación del Marco Civil, otras legislaciones ya habían sido usadas para hacer valer cuestiones relativas a la protección de datos y ya estaban siendo construidas para darle continuidad a lo que sería la LGDP. Por ejemplo, el Código del Consumidor (CDC), fechado en 1990, dispone en su Artículo 43 que:

> El consumidor [...] tendrá acceso a la información existente en suscripciones, fichas, registros y datos personales y de consumo archivados sobre él, así como sobre sus respectivas fuentes. Las suscripciones y datos de consumidores deben ser objetivos, claros, verdaderos y en un lenguaje de fácil comprensión, y no pueden contener información negativa referente a un periodo superior a cinco años.

También afirma que el consumidor podrá exigir la corrección de los datos que sean inexactos. Pese a ser proyectada durante un periodo en el que Internet comercial todavía no planteaba los desafíos relativos a la privacidad de hoy en día, el CDC ya proporcionaba un insumo que podría ser usado, aunque de forma tangencial, para proteger al usuario.

La LGDP, por su parte, comenzó a ser debatida en 2010, cuando el Ministerio de Justicia promovió una consulta pública sobre el tema, y culminó en el envío, por parte del Gobierno Federal de un proyecto de ley para el Congreso Nacional. Este proyecto se acumuló con otras proposiciones que ya estaban en debate, y fue discutido en Comisiones Especiales. Después de dos años de debates, repletos de audiencias públicas y consultas, el temario fue aprobado y sancionado en 2018. La ley solucionó los eventuales conflictos entre las normas existentes y acercó a Brasil con la tendencia internacional de establecer una ley general de protección de los datos personales.

Cabe agregar que, a fines de 2019, el Gobierno brasileño emitió dos decretos: 10.046 y 10.047 /2019, que prevén la gobernanza y el intercambio de datos personales dentro del alcance de la administración pública federal e instituyen el Registro de la Base Ciudadana y el Comité Central de Gobierno de Datos. Aunque la propuesta inicial de

los decretos es proponer una mayor armonía entre las actividades de procesamiento y recopilación de datos personales del gobierno, el texto promueve la confusión y ofrece nuevas definiciones para algunos de los conceptos tratados en el LGPD. Ambos decretos son objeto de debates en el Congreso Nacional de Brasil que proponen su derogación.

3.2. Puntos principales de la Ley de Protección de Datos respecto de las prácticas de las cuatro EMNBD seleccionadas

A continuación, teniendo en cuenta las prácticas presentadas en las políticas de privacidad y los términos de servicio de las 4 EMNBD seleccionadas, se analizará su compatibilidad con la ley que entrará en vigencia en agosto de 2020 y si esta es suficiente para enfrentar sus desafíos.

3.2.1. Finalidad, consentimiento y compartir información con terceros

Específicamente, la LGDP definió los datos personales como información relacionada con la persona natural identificada o identificable. En el Artículo 6, enumeró una serie de principios que deberán guiar el tratamiento de tales datos. Según este artículo, estos son finalidad, adecuación, necesidad, libre acceso, calidad de datos, transparencia, seguridad, prevención, no discriminación y responsabilidad y rendición de cuentas.

Además de esos principios, la ley dispone que el consentimiento es requisito para el tratamiento de los datos personales por parte del sector privado, a no ser en el caso de cumplimiento de una obligación legal y otras excepciones puntuales, como los casos de legítimo interés del controlador. En ese caso específico, la ley dispone que "cuando el tratamiento esté basado en el legítimo interés del controlador, solamente los datos personales estrictamente necesarios para la finalidad pretendida podrán ser tratados" (Artículo 10, parágrafo 1). La ley también dispone en el parágrafo 5° del Artículo 7 que el controlador que obtenga consentimiento y que requiera comunicarse o compartir datos con otros controladores, deberá obtener el consentimiento específico para esos fines (también salvaguardadas las hipótesis de dispensa de consentimiento).

La ley también dispone que el consentimiento debe destacarse de las demás cláusulas contractuales y debe referirse a finalidades determinadas, pudiendo ser revocado en cualquier momento. Siendo que el

titular también tiene derecho al acceso facilitado a la información sobre el tratamiento de sus datos, en relación con:

a. finalidad específica del tratamiento;
b. forma y duración del tratamiento, observados los secretos comercial e industrial;
c. identificación del controlador;
d. información de contacto del controlador;
e. información acerca del uso compartido de datos por parte del controlador y la finalidad;
f. fresponsabilidades de los agentes que realizarán el tratamiento; y
g. derechos del titular, con mención explícita a los derechos contenidos en el artículo 18 de esta Ley.

Respecto de las prácticas de las empresas analizadas a la luz de lo que dice la LGDP sobre el consentimiento, los datos compartidos con terceros y los principios, algunos aspectos merecen atención.

En relación con Social Miner, por ejemplo, no hay claridad respecto de la forma como se da el consentimiento del usuario para que sus datos pasen a integrar la base de datos de la empresa. El consentimiento para la recolección de los datos de navegación, amparados en la recolección de *cookies*, se da con la aceptación por parte de los usuarios en las páginas web de cada cliente de Social Miner, a partir de las notificaciones que aparecen en las esquinas superiores o inferiores de la pantalla. Sin embargo, no se sabe si hay un patrón de texto informado a los usuarios en las páginas web de cada cliente o si las notificaciones de rastreo de *cookies* son específicas o suficientes para que el usuario comprenda que la recolección será usada no solo para mejorar la navegación, sino también con fines claros de marketing digital.

Además, la política de privacidad afirma que los avisos de recolección de datos "podrán aparecer al final de la navegación de cada usuario o al inicio, cuando el mismo demuestre la intención de salir del sitio web del cliente, de tal forma que no se perjudique la navegación o se impidan eventuales procedimientos de compra" (Social Miner s.a. c). Siempre y al inicio de la navegación, los usuarios deberían ser informados sobre la posibilidad de recolección de sus datos, de tal forma que logren una mayor y más rápida comprensión sobre esta.

Además de eso, la empresa presenta fuertes disposiciones en relación con los datos compartidos con terceros. Según la política de privacidad,

"además de la propia Social Miner, ninguna otra empresa o cliente tendrá acceso a los datos e información personal de sus leads. Estamos en contra de la política de *Cookiepool* y jamás compartiremos la base entre nuestros clientes" (Social Miner s.a. c). Esta disposición es adecuada, pues tiene en cuenta la privacidad de los usuarios, pero podría haber sido incluida en la política de privacidad debido a la propia presión del mercado de marketing amparado en las *cookies* que rechaza la noción de *cookiepool*.

Las demás empresas analizadas también presentan puntos críticos respecto del consentimiento y datos compartidos con terceros. En el caso de Amazon Prime Video, esto es aún más complejo, comenzando por la dificultad de encontrar las políticas de privacidad que rigen ese servicio, cuando es contratado mediante una operadora de telefonía. Según el contrato con Vivo, el servicio está regido por los términos de uso de ambas empresas. Pero los términos de uso para la suscripción del Prime Video por parte de los clientes de Vivo no disponen nada sobre la protección de datos de los que contrataron ese servicio, pues solo versan sobre las formas de contratación, la forma de pago y la cancelación. La información sobre la privacidad y seguridad que tienen que ver con el plan de celular o de banda ancha están disponibles en la página del Centro de Privacidad de Vivo (Vivo s.a. a), pero no hay información sobre el servicio específico de Amazon Prime Video.

En los términos de uso de Amazon Prime Video, que se encuentran en un *hiperlink* en el contrato con la Vivo, los clientes también verán un *link* para el Aviso de Privacidad (*Privacy Notice*) y la política de anuncios de Amazon, pero todos están en inglés, o sea que solo con una insistencia investigativa los consumidores llegarían a las políticas de privacidad de Vivo y de Amazon y, en el caso de Amazon, tendrían que saber inglés para entenderla, a pesar de que el servicio se ofrezca en Brasil y en asocio con una empresa establecida en este país. Esas circunstancias no solo imposibilitan un consentimiento informado, sino que también dificultan cualquier acceso a la información o al control de uso de datos por parte de los consumidores.

Además de esa dificultad de entender cuáles políticas de privacidad se aplican, cuáles son las empresas controladoras y qué tipos de datos son objeto de tratamiento, tanto la política de privacidad de Vivo como el Aviso de Privacidad de Amazon abren márgenes para que más actores tengan acceso a los datos de sus consumidores. Ahora bien, si partimos de que el consentimiento se informa con dificultad en lo que atañe al

tratamiento de datos por parte de esas empresas, la situación empeora aún más cuando hablamos de los datos compartidos con terceros.

El Aviso de Privacidad de Amazon (Amazon 2017), al responder a la pregunta: "¿Amazon comparte la información que recibe?", anuncia que la "empresa no vende información de sus clientes", pero enumera los actores con los que comparte esos datos. Entre ellos están lo que el Aviso de Privacidad denomina *"affiliated businness we do not control"* (o sea, negocios afiliados de los cuales no tenemos control), pero no se especifica quiénes serían esos afiliados, pues el texto solo remite a otro texto en donde tenemos algunos ejemplos de marcas, principalmente, norteamericanas, tales como Starbucks, OfficeMax, Verizon Wireless, Sprint, T-Mobile, AT&T, J&R Electronics, Eddie Bauer y Northern Tool + Equipment. Podría asumirse que Vivo también entraría en esa categoría. Finalmente, también afirma que, en el caso de compra o venta de los negocios de Amazon, "la información de los consumidores es considerada como un activo del negocio que es transmitida", pese a que se afirme que continuarían las políticas de privacidad previas a la venta. Todas esas previsiones abren brechas enormes para cuestionarnos respecto del principio de la finalidad y el consentimiento del consumidor acerca del uso de sus datos.

Por su parte, iFood dice que los "integrantes del grupo ifood" y "los proveedores de servicios y otros socios" pueden tener acceso a los datos de los clientes (iFood 2018). La política es amplia y no deja claro cuáles datos podrían ser compartidos, dando a entender, inclusive, que la empresa podría tercerizar los servicios de iFood para las subsidiarias y, en consecuencia, su base de usuarios. También afirma que los datos compartidos con terceros, para fines de *marketing*, solo ocurre cuando ese tercero tiene patrones de protección de la privacidad similares a los del propio iFood, pero no detalla exactamente cuáles tipos de datos podrán ser compartidos. Partiendo de esto, no es posible evaluar si tales datos serían los estrictamente necesarios para los fines de *marketing*, o si ellos extrapolan tal objetivo. En todo caso, la política no es específica o suficiente y parece abrirle a un foro muy amplio la posibilidad de accesos de la base de usuarios del servicio.

Por su parte, Magazine Luiza posee una política de privacidad relativamente omisa en relación con la obtención del consentimiento de los usuarios. El documento solo dispone acerca de la utilización de los datos y una posterior posibilidad del cliente para suspender la suscripción de

la base de datos de los correos electrónicos de *marketing* y no sobre la obtención de la autorización previa, informada y consentida que oriente el tratamiento de los datos. En lo que se refiere a los datos compartidos, la política de privacidad dispone que "no se compartirá, venderá o presentará los datos de los Usuarios con terceros que no sean sus socios" (Magazine Luiza 2015). Así como en los otros casos que mencionamos aquí, la política de Magazine Luiza sigue siendo amplia y no dispone sobre quiénes serían sus eventuales socios y ni si se compartirán los datos con fines de *marketing*.

3.2.2. Uso de cookies

Además de compartir con terceros, las 4 empresas afirman que utilizan *cookies* y diferentes tipos de *webtrackers*. Al contrario de lo que dispone la Regulación General de Protección de Datos (*General Data Protection Regulation*–GDPR), la legislación brasileña no tiene disposiciones específicas para el uso de esas tecnologías. Sin embargo, se puede hacer la pregunta acerca de cómo el uso de *cookies* y de tecnologías similares de rastreo podrían empalmarse en los principios de la finalidad, adecuación, necesidad e incluso de la no discriminación, todos previstos por la ley brasileña.

Entre las empresas analizadas, Social Miner es la única que tiene una política específica de *cookies*, algo esperado si consideramos que los servicios prestados por la *start-up* se encuentran en gran parte basados en el rastreo de *cookies* con fines de la campaña de *marketing*. Esa política explica en qué consisten y cuáles son los tipos de *cookies* recolectados por la empresa.

La propia política de privacidad de Social Miner cita a la GDPR, con el fin de disponer que la *start-up* estaría de acuerdo con lo que dice el reglamento europeo. La presencia de tal indicativo es loable. Pero, aun así, la política afirma que es responsabilidad del cliente de Social Miner informar a los usuarios sobre la recolección de *cookies* y datos personales (en el caso de conexión por medio de correo electrónico o de redes sociales), algo que es comprensible desde el punto de vista operacional, pero que deja al usuario en una situación de vulnerabilidad por depender de los patrones de transparencia del cliente (contratante de Social Miner).

Por su parte iFood determina que la información sobre las actividades de los usuarios en el sitio web o en la aplicación de la empresa es

agregada y considerada como datos "no personales", pues supuestamente no permite la identificación de cada usuario. La política también clasifica "la edad del individuo, las preferencias individuales, el idioma, el CEP y el código de área" como "datos no personales" (iFood 2018). Tales clasificaciones pueden indicar un intento por excluir de la protección legal a ese tipo de información, pues se refieren a los datos que claramente son personales y que, sin el debido tratamiento, pueden fácilmente ser usados para identificar a los individuos específicos. Así, es grave la disposición de iFood en el sentido de intentar clasificar ciertos datos como no personales, y deja las puertas abiertas para una potencial violación de la privacidad de los clientes de la empresa.

En cuanto a la recolección de las *cookies* de los usuarios de los servicios estudiados, cabe precisar que estos datos sirven como identificadores generados o recolectados sobre un usuario. Al adoptar el concepto de dato personal como "información relacionada con la persona natural identificada o identificable" (Brasil 2018), se puede decir que la LGDP considera que la *cookie* actúa como un identificador electrónico (Gomes 2018), o que tiene el objetivo de inferir los perfiles de compra, como una forma de recoger los datos personales.

Además, la política de privacidad de iFood dice que "en algunos de nuestros mensajes de e-mail, (iFood usa) una '*URL click-through*' (dirección externa) vinculada al contenido de iFood. Cuando los clientes dan un clic en una de esas URL, los usuarios son enviados a un servidor diferente antes de llegar a la página de destino de nuestro servicio. iFood monitorea esos datos de *click-trhough* para entender el interés en determinados tópicos y para evaluar la eficacia de la comunicación con nuestros clientes" (Gomes 2018). En caso de que el cliente no quiera ser monitoreado, la política demanda que él "no de un clic en el texto o en los *links* contenidos en mensajes de *e-mail* enviados por iFood" (Gomes 2018).

Aparentemente, la práctica de direccionamiento de los usuarios a los servidores antes de la página final de destino no se les informa a los clientes en ningún momento —salvo a aquellos que lean la totalidad de la política de privacidad antes de dar clic en algún *link* vehiculado por iFood en sus correos enviados a los clientes—. Tal práctica no es ideal y puede vulnerar los derechos de los usuarios de consentir con claridad respecto de la recolección de sus datos.

En el caso de Magazine Luiza, la política de privacidad de la aplicación (Magazine Luiza 2015) presenta un punto específico sobre las

cookies en donde se dispone que el sitio web/la aplicación podrán hacer uso de estas, y que el usuario puede deshabilitarlas. El documento explicita que se realizarán recomendaciones de productos a partir de una *cookie* que identifica la navegación del usuario. En este caso, la navegación engloba el comportamiento del usuario dentro del sitio web/la aplicación enfocándose en factores como: 1) si hubo navegación o compra; 2) ítems visualizados, investigados o comprados; 3) los demás usuarios en situaciones similares (Magazine Luiza 2015).

El aviso de privacidad de Amazon también trata específicamente sobre *cookies*, al indicar la posibilidad de deshabilitarlas en el *browser*, pero, al mismo tiempo indica que "si usted bloquea o rechaza nuestras *cookies*, no será posible adicionar ítems en su carrito, hacer el *checkout* y tampoco usar ningún producto de amazon.com que requiera que usted se suscriba". De tal forma que, aunque existe la posibilidad de deshabilitar las *cookies*, es imposible hacerlo y continuar usando los servicios de Amazon. Cabe resaltar que existen diferentes tipos de *cookies*, con diferentes funcionalidades, por lo que sería técnicamente posible distinguirlas y habilitar solo las necesarias para el funcionamiento de la plataforma.

3.2.3. ¿La relación con GAFAM puede darse en el tratamiento no autorizado de datos sensibles?

En relación con los datos personales sensibles, definidos por la ley como un "dato personal sobre el origen racial o étnico, convicción religiosa, opinión política, afiliación a un sindicato o a una organización de carácter religioso, filosófico o político, dato referente a la salud o a la vida sexual, dato genético o biométrico, cuando están vinculados a una persona natural" (Artículo 5, inciso 2), la LGDP incluso afirma que los "datos anonimizados no serán considerados datos personales [...], salvo cuando el proceso de anonimización al cual fueron sometidos sea revertido utilizando exclusivamente medios propios, o cuando, con esfuerzos razonables, pueda ser revertido". O sea, el tratamiento de los datos que no generen la identificación de los titulares posee una ventana de exploración y posibilidades mayores.

Las relaciones de las empresas estudiadas con las empresas GAFAM y, por lo tanto, con otras bases de datos, abren un margen para el acceso a los datos sensibles de sus clientes. Sin embargo, ninguna de las políticas de privacidad estudiadas mencionan explícitamente el tratamiento de esos datos, aunque varias de ellas hagan alguna actividad de *profiling*.

3.2.4. Derecho de acceder con facilidad, corregir o borrar información

La LGDP también garantiza al titular el derecho de acceder con facilidad a la información sobre la finalidad del tratamiento de los datos, la duración y la forma de este, la información sobre el controlador de los datos y sobre los que se comparten con terceros.

Hay disposiciones en la política de privacidad de Social Miner en relación con la información compartida con terceros y la finalidad de los datos, pero no es clara la duración del almacenamiento de los datos de los usuarios, y tampoco hay disposiciones que detallen cómo estos pueden pedir correcciones o que sus datos sean borrados de la base.

iFood, por su parte, afirma que podrá almacenar los datos mientras sea necesario para los fines de la política de privacidad y del cumplimiento de los términos de uso, "respetando el periodo de retención de datos determinado por la legislación aplicable" (Magazine Luiza 2015). También afirma que los usuarios podrán solicitar la exclusión de la cuenta, pero no muestran cómo puede ser realizada tal petición. En todo caso, dispone que:

> En algunos casos, (iFood podrá) retener su información, inclusive si usted ha eliminado su cuenta, tal como en la hipótesis de salvaguarda obligatoria de registros prevista en la ley aplicable, en el caso de que haya un asunto no resuelto en relación con su cuenta (como, por ejemplo, una queja o disputa no resuelta), o en el caso de que sea necesario para nuestros intereses comerciales legítimos, como prevención de fraudes y mejora de la seguridad de nuestros usuarios (iFood 2018).

La retención de datos para los intereses comerciales legítimos abre un espacio para muchas posibilidades, dada la vaguedad del término utilizado, y puede generar almacenamientos onerosos y abusivos para los usuarios. Además de eso, según la política, pueden ser usados los *feedbacks* enviados por los clientes sobre las entregas de iFood, para fines de publicidad y publicados en el sitio web y en la aplicación de la plataforma. Sin embargo, no se sabe si hay claridad para los usuarios en términos de la visibilidad irrestricta de sus *feebacks* más allá de la disposición en la política de privacidad.

Magazine Luiza le da un tratamiento al usuario como titular de hecho de los datos y le permite la adición, exclusión o modificación de

información vinculada a su perfil de usuario (Magazine Luiza 2015). A pesar de que el documento dispone la garantía del derecho del usuario a acceder, corregir o borrar su información, este no menciona cuáles medios podrán ser utilizados para ello. Sobre este punto, la política de privacidad no trata sobre la posibilidad de exclusión de los datos después del término de la relación que motivó su recolección, y tampoco menciona el periodo de tratamiento de los datos personales del usuario.

En el caso de Amazon Prime Video, la *Privacy Notic*e dice que se puede ingresar informaciones sobre la cuenta "con el propósito limitado de visualizarlas" y, en algunos casos, actualizarlas. El documento también dice que se pueden ver algunos ejemplos, pero el *link* nos direcciona nuevamente a la *Privacy Notice*. De nuevo, se ve con aprehensión el hecho de que el servicio de *streaming* no tiene una política de privacidad específica, pues el proceso de *profiling* para un servicio de *streaming* de videos es distinto, por ejemplo, del *profiling* hecho para la compra y venta de productos.

Se consideran los casos como el señalado por un artículo del New York Times (Fisher, Taub 2019) que, al investigar el sistema de recomendaciones y búsquedas de Youtube en Brasil, demostró que la plataforma tiende a direccionar a los usuarios hacia canales de extrema derecha. Es necesario, por lo tanto, pensar en qué tipo de transparencia se puede exigir, de ese y de otros tipos de servicios *streaming* que, cada vez más, hacen uso de la inteligencia artificial para hacer recomendaciones. Finalmente, tampoco se encuentra nada que mencionara explícitamente la posibilidad de la exclusión de los datos.

3.2.5. La práctica de profiling y el potencial de discriminar por algoritmos

En relación con las prácticas de *profiling*, la LGDP no es muy clara. En su Artículo 5°, la ley traza definiciones de dato personal, dato personal sensible y dato anonimizado[7] y describe que la anonimización de datos es la utilización de "medios electrónicos razonables y disponibles en el

---

7 Art. 5º Para los fines de esta Ley, se considera:
I - dato personal: información relacionada con la persona natural identificada o identificable;
II - dato personal sensible: dato personal sobre el origen racial o étnico, convicción religiosa, opinión política, filiación a un sindicato o a una organización de carácter religioso, filosófico o político, dato referente

momento del tratamiento, por medio de los cuales un dato pierde la posibilidad de asociación, directa o indirecta, a un individuo". Además de eso, la ley autoriza el tratamiento de datos personales para la realización de estudios por el órgano de investigación, siempre que sea posible la anonimización de la información (Art. 7°, inc. IV).

Otro punto importante es que la LGDP no considera a los datos anonimizados como datos personales, a no ser que el proceso de anonimización pueda ser revertido[8]. El mismo Artículo 12 describe que podrán ser considerados como datos personales aquellos utilizados para la formación de perfiles comportamentales de la persona natural, si está identificada, y que le compete a la Autoridad nacional de protección de datos personales disponer sobre "los patrones y las técnicas utilizados en procesos de anonimización y realizar verificaciones acerca de su seguridad".

En ese sentido, en el caso de que las prácticas de *profiling* trabajen con los datos anonimizados, estas no representan una violación de la LGDP. Adicionalmente, la Ley no define lo que serían los "esfuerzos razonables y por medios propios" (Soares 2018) aplicables a los procesos de reversión de los procesos de anonimización, ni tampoco los patrones mínimos para las empresas.

---

a la salud o a la vida sexual, dato genético o biométrico, cuando está vinculado a una persona natural;
III - dado anonimizado: dato relativo al titular que no pueda ser identificado, considerando la utilización de los medios técnicos razonables y disponibles con ocasión de su tratamiento.

8 Art. 12. Los datos anonimizados no serán considerados datos personales para fines de esta Ley, salvo cuando sea revertido el proceso de anonimización al cual fueron sometidos, utilizando exclusivamente medios propios, o cuando, con esfuerzos razonables, pueda ser revertido.
§ 1° La determinación de lo que sea razonable debe tener en cuenta factores objetivos, tales como el costo y el tiempo necesarios para revertir el proceso de anonimización, de acuerdo con las tecnologías disponibles, y la utilización exclusiva de los medios propios.
§ 2° Igualmente podrán ser considerados como datos personales, para los fines de esta Ley, aquellos utilizados para la formación del perfil comportamental de determinada persona natural, en caso de estar identificada.
§ 3° La autoridad nacional podrá disponer sobre los patrones y las técnicas utilizados en los procesos de anonimización y realizar verificaciones acerca de su seguridad, una vez oído el Consejo Nacional de Protección de Datos Personales.

En términos generales, no fue posible concluir si la actividad de las empresas analizadas en el presente estudio influía sobre las prácticas de *profiling* o las eventuales discriminaciones generadas por decisiones algorítmicas.

La política de privacidad de iFood afirma que la empresa realiza una clasificación de los clientes conforme los eventos realizados. Por ejemplo, clasifican a los usuarios que "piden más determinada categoría de comida o que realizan más de 4 pedidos por mes" (iFood 2018). Sin embargo, no se sabe cuáles son los usos específicos y detallados de tales clasificaciones, que pueden generar vulnerabilidad para los usuarios en la medida en que ofrecen parámetros claros de preferencias y costumbres personales.

La operación de Social Miner, a su vez, está basada en el análisis del comportamiento de compra del usuario hecha automáticamente por el algoritmo de la *start-up*. Sin embargo, no hay indicaciones sobre el funcionamiento de tal algoritmo y de las potenciales categorizaciones de usuarios en grupos conforme al patrón de compras, lo que, una vez más, deja al usuario en situación de vulnerabilidad y de potencial sobreexposición. La empresa afirma que hace estudios sobre los patrones consumidores. En ese caso, "tales datos tendrán la información personal borrada de los usuarios, que ya no se configuran como un dato personal, y sí como un mero conjunto de datos anónimos para fines de estudio e investigación" (Social Miner s.a. c). Aun así, indica que existe, en alguna medida, la creación de perfiles según los datos de los usuarios.

La política de Privacidad de MagaLu también es omisa en relación con las eventuales prácticas de *profiling* practicadas por la empresa y las estrategias de direccionamiento de contenido o de clusterización de clientes. Todo lo que el documento menciona es la eventual utilización de una *cookie* que identifica la navegación del usuario para la posterior recomendación de productos que será diferenciada para cada comportamiento dentro del sitio web. El documento también menciona que la recomendación de productos será "generada a partir de algoritmos, su precisión puede no ser exacta, sin embargo, busca sugerir productos que sean del interés del usuario, sin que este tenga cualquier obligatoriedad de adquirirlos".

Amazon Prime Video ha contratado a especialistas de análisis de datos para mejorar su algoritmo, pero sus términos de servicio y política

de privacidad no dicen mucho sobre cómo funciona eso ni tampoco sobre cómo se puede intervenir. Inclusive porque las políticas de privacidad son genéricas y se refieren a todos los servicios de Amazon, y no específicamente al de Amazon Prime Video. En la política específica, solo se encontró mención al software, diciendo que él puede suministrarle a Amazon la:

> Información relacionada con su uso y con el desempeño del servicio y del software, así como la información referente a los dispositivos en los cuales usted baja y utiliza el servicio de software. Por ejemplo, el software podrá suministrarle a Amazon información relacionada con el contenido digital que usted baja o al que accede a través de *streaming* y su uso de ese contenido digital (como, por ejemplo, se usted visualizó un contenido digital y cuándo lo hizo, lo que podrá, entre otras cosas, ayudarnos a medir el periodo de acceso al contenido digital alquilado).

Pero no hay información sobre cómo son utilizados esos datos ni sobre el poder del consumidor de editar directamente el perfil que Amazon le atribuye.

3.2.6. Otros asuntos abordados por la LGDP

Además de eso, la ley trae una disposición específica sobre el tratamiento de los datos personales de los niños y los adolescentes. Para eso, según la LGDP, es necesario el consentimiento específico de uno de los padres o responsables legales. La excepción se hace cuando "sea necesaria la recolección para contactar a los padres o al responsable legal", debiendo ser utilizada "una única vez y sin almacenamiento, o para su protección, y en ningún caso podrán ser traspasados a un tercero sin el consentimiento" (Artículo 14, parágrafo 3).

Teniendo en cuenta la importancia de prestar atención a la transferencia internacional de datos, pues muchos recursos y aplicaciones de Internet transitan por países y legislaciones muy diversas, la LGDP defiende que tal transferencia sólo podrá darse "en los países y organismos internacionales que proporcionen un grado de protección de datos personales adecuado al previsto (en la) Ley" y "cuando el controlador ofrezca y compruebe las garantías de cumplimiento de los principios, los derechos del titular y del régimen de protección de datos previstos

(en la) Ley" (Artículo 33, incisos 1 y 2). O sea que la ley brasileña sigue el patrón adoptado por el reglamento europeo (GDPR), permitiendo la transferencia solo para los países que tengan salvaguardas similares al patrón brasileño de protección de los datos.

Específicamente, en relación con los controladores y operadores, o sea, a quienes les competen las decisiones sobre el tratamiento de los datos personales y a quienes las ejecutan potencialmente en nombre del controlador, la LGDP afirma que ambos requieren mantener el registro de las operaciones que realizan, de tal forma que se guarde la memoria del tratamiento de los datos. Esa memoria debe contener, como mínimo, "la descripción de los tipos de datos recolectados, la metodología utilizada para la recolección y para la garantía de la seguridad de la información y el análisis del controlador en relación con las medidas, salvaguardas y mecanismos de mitigación de riesgo adoptados" (Artículo 39, parágrafo único).

En el caso de que haya daño patrimonial, moral, individual o colectivo, en razón del tratamiento de los datos personales, los controladores y/o operadores están obligados a repararlos, según las medidas judiciales. Además de eso, la ley deja claro que "el operador responde solidariamente por los daños causados por el tratamiento cuando se incumplan las obligaciones de la legislación de protección de datos o cuando no hayan seguido las instrucciones lícitas del controlador", y que "los controladores que estuvieran directamente involucrados en el tratamiento del cual resulten daños al titular de los datos respondan solidariamente" (artículo 42, parágrafo 1, incisos 1 y 2), inclusive cuando el daño resulte del descuido de ambos en relación con la adopción de medidas adecuadas de seguridad.

4. Evaluación de la capacidad de la Autoridad Nacional de Protección de Datos Personales para tratar con las EMNBD

La Autoridad nacional de protección de datos personales brasileña (ANPD) fue aprobada por disposición de la sanción de la Ley 13.583 del 8 de julio de 2019, 11 meses después de la aprobación de la Ley General de Protección de Datos Personales. Sin embargo, el modelo de Autoridad de protección de datos personales adoptado por Brasil dista de ser el deseado por algunos sectores involucrados en la discusión de la Ley, ya

que el órgano hará parte de la administración pública directa y vinculado a la Casa Civil de la Presidencia de la República.

Cabe destacar que las discusiones relacionadas con la aprobación de la LGDP en el Congreso Nacional involucraron un modelo de autoridad independiente, con autonomía decisoria, institucional y financiera, capaz de implementar y acompañar la aplicación de la Ley. La legalidad de la creación de la ANPD, como una autarquía, fue un punto bastante cuestionado pues las especificidades del modelo fueron añadidas en el texto de la Ley en el transcurso del debate legislativo. Los argumentos en torno de la ausencia de legalidad en la creación de la ANPD en la discusión de la ley influyeron sobre la decisión del Poder Ejecutivo, que entendió que el Congreso Nacional estaba violando la competencia exclusiva de la Presidencia de la República para legislar sobre la organización de la Administración Pública Directa e Indirecta y acabó vetando los dispositivos referentes a la ANPD.

Sin embargo, el 27 de diciembre de 2018, fue editada la Medida Provisoria n. 869/2018 que, al ser sancionada como Ley 13.853/2019 alteró la Ley de Protección de Datos y volvió a agregar en el texto de la LGDP la previsión de la creación de la ANPD como órgano de la administración pública federal integrante de la Presidencia de la República, reconociendo que los vetos representaban un "riesgo de inseguridad jurídica para la Sociedad Civil ante la falta de definición del órgano responsable de la regulación, control y fiscalización de la aplicación de la Ley" (Brasil 2018).

Las funciones de la autoridad están definidas en el Artículo 55-J[9] que, en resumen, son: a) fiscalizar el cumplimiento de la ley de protección

9 Entre las más relevantes estarían: a. velar por la protección de los datos personales, en los términos de la legislación; [...] c. celaborar directrices para la Política Nacional de Protección de Datos Personales y de la Privacidad; d. fiscalizar y aplicar sanciones en el caso del tratamiento de datos realizado en incumplimiento de la legislación, mediante el proceso administrativo que afirme lo contrario, la amplia defensa y el derecho de recurso; [...] f. divulgar entre la población el conocimiento de las normas y de las políticas públicas sobre la protección de datos personales y de las medidas de seguridad; g. promover y elaborar estudios sobre las prácticas nacionales e internacionales de protección de datos personales y privacidad; (...) i. promover acciones de cooperación con las autoridades de protección de datos personales de otros países, de naturaleza internacional o transnacional; [...] m. editar reglamentos

de datos; b) fiscalizar y aplicar sanciones; c) apreciar peticiones de titulares de datos (ciudadanos) en contra de los controladores; d) elaborar estudios; e) estimular la adopción de servicios "*privacy friendly*"; f) cooperar con las autoridades de protección de datos de otros países; g) solicitar informes e disponer sobre las formas de publicitar las operaciones de tratamiento; h) hacer estudios y editar reglamentos; i) realizar auditorías o determinar su realización; j) comunicar las infracciones a las autoridades competentes.

La ANPD es responsable de la elaboración de directrices para una Política Nacional de Protección de Datos Personales y Privacidad, fiscalización de las actividades del tratamiento de datos personales y la aplicación de eventuales sanciones a los agentes que violen los derechos establecidos en la ley.

En el transcurso del debate legislativo fue agregada la competencia de:

> Editar normas, orientaciones y procedimientos simplificados y diferenciados, inclusive en cuanto a los plazos, para que las microempresas y empresas de pequeño porte, así como las iniciativas empresariales de carácter incremental o disruptivo que se declaren a sí mismas como start-ups o empresas de innovación, se puedan adecuar a esta Ley.

El legislador intentó prever una especie de escalonamiento de la aplicación de la Ley para los *start-ups* y las empresas disruptivas. El desafío presentado para la ANDP, por lo tanto, es la delimitación de las reglas y los plazos para la adecuación de los *start-ups* que equilibren el derecho

---

> y procedimientos sobre la protección de los datos personales y la privacidad, así como sobre informes de impacto para la protección de datos personales para los casos en que el tratamiento represente un alto riesgo para la garantía de los principios generales de protección de datos personales previstos en esta Ley; [...] q. editar normas, orientaciones y procedimientos simplificados y diferenciados, inclusive en cuanto a los plazos, para que las microempresas y las empresas de pequeño porte, así como las iniciativas empresariales de carácter incremental o disruptivo que se declaren a sí mismas startups o empresas de innovación, puedan adecuarse a esta Ley; [...] s. deliberar, en la esfera administrativa, con carácter terminante, sobre la interpretación de esta Ley, sus competencias y los casos omisos; [...]

a la privacidad y la protección de datos con el fomento a la innovación sin debilitar el régimen jurídico recién conquistado.

La Ley, en su Artículo 52, dispone sobre las sanciones aplicables a los agentes de tratamiento de Datos (advertencia, multa simple, multa diaria, bloqueo y eliminación de datos personales). Estas no sustituyen la aplicación de sanciones administrativas, civiles o penales en la legislación específica.

A pesar de la importancia de la creación de una Autoridad de Protección de Datos Personales, el arreglo institucional para el ejercicio del poder de fiscalización no es el ideal. Así lo anotó Bruno Bioni en una entrevista que le concedió al *Jornal O Estado de São Paulo*. Por ejemplo, el veto a la posibilidad de aplicación de las sanciones administrativas a los agentes de tratamiento de datos referentes a:

> "(a) Suspensión parcial del funcionamiento del banco de datos al que se refiere la infracción por el periodo máximo de 6 (seis) meses, prorrogable por igual periodo, hasta la regularización de la actividad de tratamiento por parte del controlador; (b) Suspensión del ejercicio de la actividad del tratamiento de los datos personales al que se refiere la infracción por el periodo máximo de 6 (seis) meses, prorrogable por igual periodo; y (c) Prohibición parcial o total del ejercicio de actividades relacionadas con el tratamiento de los datos" (Brasil 2019).

De acuerdo con el texto de la Ley, la aplicación de las sanciones administrativas descritas arriba solo ocurrirá ante la reincidencia de una determinada empresa o entidad de la administración pública. O sea que la aplicación de los dispositivos solamente podría ocurrir después de la imposición de por lo menos una sanción administrativa de las descritas la lista del Artículo 52 o en el caso de los controladores sometidos a otros órganos y entidades con competencias sancionatorias, una vez oídos estos órganos.

Es importante mencionar que las sanciones arriba descritas eran fundamentales para el fortalecimiento y el poder de fiscalización y control de la Autoridad Nacional de Protección de Datos Personales, cuando una autoridad fuerte, con el poder de sanción reforzado se vuelva relevante para impedir los abusos cometidos por los agentes de tratamiento de los datos personales. Sin embargo, se puede decir que el modelo de autoridad brasileño será insuficiente, pues el órgano nace desprovisto

de autonomía —la ley garantiza la autonomía técnica y decisoria, pero la financiera e institucional todavía están pendientes de una eventual revisión—.

El tamaño de la ANPD también es bastante modesto, está compuesto por un consejo rector, con cinco miembros, y un Consejo Nacional de Protección de Datos Personales y Privacidad conformado por 23 integrantes. Sin embargo, la estructura de la ANPD todavía es desconocida en la medida en que la ley solo informa que el órgano contará con una interventoría, una auditoría, un órgano propio de asesoría jurídica y las eventuales unidades administrativas y unidades especializadas necesarias para la aplicación de la Ley (Art. 55-C).

La propuesta de autoridad mejora con la creación del Consejo Nacional de Protección de Datos Personales (Art. 58-A). El órgano multisectorial compuesto por 23 representantes del sector público, privado, tercer sector y de la academia, permite una participación más efectiva de los sectores interesados en la actividad de la ANPD. De acuerdo con la Ley (Art. 58-B), el CNPD es responsable de: 1) elaborar directrices estratégicas y suministrar subsidios para la elaboración de la Política Nacional de Protección de Datos Personales y de la Privacidad y para la actuación de la ANPD; 2) elaborar informes anuales de evaluación de la ejecución de la acciones de la Política Nacional de Protección de Datos Personales y de la Privacidad; 3) elaborar estudios y realizar debates y audiencias públicas; y 4) difundir el conocimiento.

En lo referente al punto de la autonomía e independencia de la ANPD, el paliativo encontrado y agregado en el texto fue la inclusión de dos parágrafos en el texto de la Ley, que indican que la naturaleza jurídica del órgano podrá ser transformada por el Poder Ejecutivo en autarquía y que ese aval deberá ocurrir en un periodo de hasta dos años después de agosto de 2020 (fecha de la entrada en vigencia de la Ley)[10].

---

10 Art. 55-A. Queda creada, sin aumento del gasto, la Autoridad Nacional de Protección de Datos (ANPD), órgano de la administración pública federal, integrante de la Presidencia de la República.

§ 1º La naturaleza jurídica de la ANPD es transitoria y podrá ser transformada por el Poder Ejecutivo en una entidad de la administración pública federal indirecta, sometida a un régimen autárquico especial y vinculada a la Presidencia de la República.

§ 2º La evaluación en cuanto a la transformación que dispone el §1º de este artículo deberá ocurrir en un período de hasta 2 (dos) años a partir

Conclusión y Recomendaciones

De manera general, las prácticas ya conocidas de EMNBD fueron identificadas en las empresas analizadas. El uso de *cookies* y de otras formas de recolección de datos de navegación, de compartir bases de datos con terceros y de direccionamiento de contenido en plataformas por medio de *profiling*, de una forma u otra, fueron identificados en las empresas analizadas por el presente estudio. Además de eso, como en el caso colombiano, también fue identificada una fuerte relación con las empresas GAFAM, bien sea por la utilización de datos de las plataformas para la autenticación o por la posibilidad de direccionamiento de contenidos en las mismas.

En relación con las cuatro empresas analizadas, la actual política de privacidad de iFood y de Magazine Luiza fueron escritas antes de la sanción de la LGDP y, por lo tanto, no hacen mención a la legislación o a las obligaciones de la ley de forma directa. De igual forma, Social Miner tampoco menciona la LGDP, pero establece claros vínculos con el reglamento europeo, afirmando que está de acuerdo con la norma europea. En cuando a Vivo, que deja disponible Amazon Prime Video, inauguró recientemente una Central de Privacidad, que, de cierta forma se acoge a los principios de la LGDP, pero la mayor parte de los datos de utilización de servicio, están regidos por el Aviso de Privacidad de Amazon, que no solo no menciona la ley brasileña, sino que únicamente está disponible en inglés.

Si se tiene en cuenta el régimen jurídico presentado y la situación actual de la autoridad nacional de protección de datos, aún es muy pronto para alegar que la regulación será lo bastante fuerte para combatir las eventuales violaciones a la privacidad y a los derechos de los ciudadanos practicadas por las empresas. La Autoridad Nacional de Datos Personales, en el modelo aprobado, aparenta ser débil y sin poder efectivo de fiscalización. En función de eso, para que la fiscalización de los agentes sea efectiva en el país, es importante que el órgano esté dispuesto a cooperar con otros sectores y órganos fiscalizadores como los pertenecientes al Sistema Nacional de Defensa del Consumidor y a la propia Justicia Federal.

---

de la fecha en que entre en vigencia la estructura que reglamentaria de la ANPD.

Por eso, se recomienda:

Para los agentes de tratamiento de datos analizados:

1. La actualización de todas las políticas de privacidad y de los términos de uso para generar la armonización con la Ley General de Protección de Datos. Las empresas requieren adecuarse a la ley brasileña, tanto en el vocabulario como en la acción, buscando dejar más claro para el usuario sus derechos garantizados por la ley y los detalles del tratamiento de sus datos personales. Queda incompleta, por ejemplo, la política de Social Miner, que cita la normativa europea en su política de privacidad varias veces, pero sin atender directamente a la legislación brasileña que pronto regirá en todo el territorio nacional.
2. La difusión de las políticas de privacidad y de los términos de uso de forma fácil, integrada y traducida a la lengua portuguesa. Por ejemplo, surgieron dificultades para entender cuál política de privacidad regía los servicios de Amazon Prime Video cuando fueron contratados por Vivo. Es esencial que las empresas suministren, según lo dispone la ley, información clara, suficiente y de fácil acceso a sus clientes o clientes potenciales y, si están involucradas dos empresas, sería fundamental un único documento que deje claro al consumidor el papel de cada una en el tratamiento de sus datos.
3. La difusión e indicación, en los términos de uso y de las políticas de privacidad, de mecanismos y/o contacto para los usuarios que deseen obtener más información referente al tratamiento de sus datos. Aunque la LGDP disponga sobre la posibilidad de que los usuarios soliciten información o modificación sobre el tratamiento de sus datos, aún es incierta en las políticas analizadas y, hay credibilidad en gran parte en las EMNBD de que el usuario tomará un camino claro siempre que desee hacer uso de sus derechos resguardados por la LGDP.
4. La instauración de políticas de gobernanza. En ninguna de las cuatro empresas analizadas se encontraron directrices que apuntaran a medidas de gobernanza o a principios orientadores del tratamiento de los datos y el cuidado de la seguridad de los usuarios. La LGDP recomienda que las empresas sean

transparentes en cuanto a sus procesos internos de gestión de datos, pero no hay, hasta el momento en las empresas analizadas, una clara ejecución de tal recomendación.

5. La obtención de detalles, por parte de las empresas sobre las medidas de seguridad adoptadas. Algunas empresas usaron términos vagos para referirse al tema, otras incluso se eximieron de la responsabilidad de resarcir a los usuarios en el caso de filtraciones y violaciones.
6. Es necesaria una mayor investigación sobre el panorama de actuación de las EMNBD en el país a partir de su incidencia sobre los derechos y las libertades de los ciudadanos. Sobre todo, teniendo en cuenta la inminencia de la aplicación de la ley, es vital para los usuarios y para las propias empresas que haya material en portugués y enfocado específicamente en el contexto brasileño sobre la relación entre las normas que inciden sobre la protección de datos personales y sobre la actuación de empresas. Tales estudios podrán, inclusive, ser utilizados por la ANPD cuando inicie sus operaciones, de tal forma que se construya un conocimiento técnico y basado en la empiria sobre el tema.
7. El uso de *cookies* y otros *trackers* también requiere ser entendido y tratado con más detalle, para que no se interprete, por patrón, que los datos que recolectan son anonimizados y, por lo tanto, que están fuera del ámbito de la protección de la ley, como se pudo ver ratificado en algunas de las políticas de privacidad.
8. A veces, se debe observar que en la relación con las empresas GAFAM, los datos sensibles están siendo recolectados, pero no se encontró mención a los datos sensibles en ninguna de las políticas de privacidad.
9. También se sugiere que el patrón para determinadas recolecciones de datos sea el *opt-in*, al contrario del *opt-out*, que ha sido el denominador común en los términos analizados.
10. Finalmente, es necesaria más claridad y transparencia sobre las prácticas de *profiling* de las empresas, ya que es un tema que no apareció explicitado con claridad en ninguna de las políticas de privacidad o en los términos de uso.

Con relación a la Autoridad Nacional de Protección de Datos

11. La revisión de modelo de la transformación de la Autoridad Nacional de Datos Personales —según lo previsto en la ley— y su posterior transformación en autarquía, perteneciente a la Administración Pública Indirecta, con independencia técnica y financiera y con fuerte poder de fiscalización es necesaria para garantizar la tutela de los derechos de los usuarios y para aplicar sanciones más severas a los agentes.
12. El derrocamiento de los vetos del Presidente Jair Bolsonaro al texto de la MP 869/2019 para restaurar las sanciones más severas incluidas en el transcurso del debate legislativo con miras a fortalecer el poder de la policía de la Autoridad (suspensiones) y dotarla de independencia Financiera.

Referencias

Amazon. *Amazon Privacy Notice*. Amazon s.a. Consultado julio 15, 2019. https://www.amazon.com/gp/help/customer/display.html?nodeId=468496

Amazon Prime Video. *Termos de Uso do Amazon Prime Video*. Amazon Prime Video s.a. Consultado julio 15, 2019. https://www.primevideo.com/region/na/help?nodeId=202095490

Baptista Luz Advogados. Proteção de dados e a legislação vigente no Brasil. Baptista Luz, 2017. Consultado en agosto 15, 2019. http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf

Barbosa, Vanessa. Até a mascote virtual do Magazine Luiza é alvo de assédio sexual. *Revista Exame*, 2018. Consultado en julio 26, 2019. https://exame.abril.com.br/marketing/ate-a-mascote-virtual-do-magazine-luiza-e-alvo-de-assedi o-sexual/

Bassette, Fernanda. A estratégia por trás do vídeo viral do Magazine Luiza. *Veja*, 2017. Consultado julio 26, 2019. https://veja.abril.com.br/blog/virou-viral/estas-vendedoras-da-magazine-luiza-estao-enlouquece ndo-a-internet/

Belloni, Luiza. Como o iFood se tornou o maior aplicativo de delivery de comida da América Latina. *Huffington Post*, 2018. Consultado julio 26, 2019. https://www.huffpostbrasil.com/2018/04/18/

como-o-iFood-se-tornou-o-maior-aplicativo-de-deliver y-de-comida-da-america-latina_a_23414651/

Bloomberg. Magazine Luiza usa Tinder para ampliar vendas e tem alta de 2000%. *Jornal O Globo*, 2017. Consultado julio 26, 2019. https://oglobo.globo.com/economia/magazine-luiza-usa-tinder-pra-ampliar-vendas-tem-alta-de-2000-21705034

Brasil. Presidência da República. Exposição de Motivos da Medida Provisória 869/2018. Consultado julio 24, 2019. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf

Brigatto, Gustavo. Movile investe US$ 500 milhões no iFood e planeja criar líder global. *Valor Econômico*, 2018. Consultado agosto 15, 2019. https://www.valor.com.br/empresas/5983273/movile-investe-us-500-milhoes-no-iFood-e-planeja- criar-lider-global

Calado, Caio. Magazine Luiza–entrevista com o time responsável pela criação da Lu. *Medium Bots Brasil*, 2018. Consultado agosto 15, 2019. https://medium.com/botsbrasil/magazine-luiza-entrevista-com-o-time-respons%C3%A1vel-pela- cria%C3%A7%C3%A3o-da-lu-8fc987fbafad

Canal da Lu–Magalu. Youtube. Consultado julio 15, 2019. https://www.youtube.com/user/MAGAZINELUIZACOM

Capelas Bruno y Renato Ghelfi. Governo sanciona MP que cria Autoridade Nacional de Proteção de Dados. *O Estado de S. Paulo*, 2019. Consultado julio 26, 2019. https://link.estadao.com.br/noticias/geral,governo-sanciona-mp-que-cria-autoridade-nacional-de-protecao-de-dados,70002913612

Congresso Nacional. (2019). Medida Provisória n. 869/2018. Consultado julio 26, 2019. https://legis.senado.leg.br/sdleg-getter/documento?dm=7966761&ts=1563991644604&dispositi on=inline

Daroit Guilherme. iFood quer seguir entregando crescimento. *Jornal do Comércio*, mayo 27, 2019. Consultado agosto 15, 2019. https://www.jornaldocomercio.com/_conteudo/cadernos/empresas_e_negocios/2019/05/685035-iFood-quer-seguir-entregando-crescimento.html

Decreto n. 10.046. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Outubro 9 de 2019. Consultado en 03/11/2020. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm

Decreto n. 10.047. Dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. Outubro 9 de 2019. Consultado en 03/11/2020. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10047.htm

Estadão. Mulher virtual da Magazine Luiza reclama de assédio em comentários. *O estado de S. Paulo*, 2018. Consultado agosto 15, 2019. https://emais.estadao.com.br/noticias/comportamento,mulher-virtual-da-magazine-luiza-reclama-de-assedio-em-comentarios,70002484761

Eveloso, Thássius. Magazine Luiza lança programa de comissão para Facebook. *Tecnoblog*, 2012. https://tecnoblog.net/74606/magazine-luiza-facebook/

Fisher Max y Amanda Taub. How Youtube radicalizes Brazil, The New York Times, agosto 11, 2019. Consultado 07/14/2019. https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

Fraga, Nayara. "Temos de ajudar o consumidor na inclusão digital", diz Trajano, do Magazine Luiza. *Época Negócios*, 2018. Consultado octubre 8, 2019. https://epocanegocios.globo.com/Empresa/noticia/2018/02/fabio-coelho-do-google-e-luiza-traja no-do-magazine-luiza-conversam-sobre-inclusao-digital.html

Freitas, Tania. As 8 startups brasileiras de machine learning que serão aceleradas pelo Google. *Startse*, 2019. Consultado octubre 8, 2019. https://www.startse.com/noticia/startups/61939/8-startups-brasileiras-launchpad-accelerator

Freitas, Tainá. iFood registra 17,4 milhões de pedidos no mês de março. *Startse*, 2019. Consultado julio 26, 2019. https://www.startse.com/noticia/startups/63248/iFood-atinge-a-marca-174-milhoes-de-pedidos-n o-mes-de-marco

Gartenberg, Chaim. YouTube is back on the Fire TV, and Prime Video launches on Chromecast starting today. *The Verge*, julio 9, 2019. Consultado octubre 8, 2019. https://www.theverge.com/2019/7/9/20686773/youtube-fire-tv-prime-video-chromecast-amazon- google-launch-today-available

Gazeta do Povo. iFood e Magazine Luiza estreiam sistema de pagamentos online do Google no Brasil. *Gazeta do Povo*, 2017. Consultado julio 26, 2019. https://www.gazetadopovo.com.br/economia/nova-economia/

ifood-e-magazine-luiza-estreiam-sistema-de-pagamentos-online-do-google-no-brasil-24pqsn32pbqozn86seh3ktp7i/

Gazzoni, Marina y Patrick Cruz. Luiza Trajano: do balcão da loja dos tios a ministra do governo. *Último Segundo-iG*, 2011. Consultado octubre 8, 2019. https://ultimosegundo.ig.com.br/politica/luiza-trajano-do-balcao-da-loja-dos-tios-a-ministra-do-go verno/n1597158849986.html

Gomes Oliveira María Cecilia. Cookie notice: informar, obter e por fim coletar dados pessoais. *JOTA*, 2018. Consultado julio 26, 2019. https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/ cookie-notice-informar-obter-e-por-fim-coletar-dados-pessoais-23112018

Google Play Store. *App do Magazine Luiza*. Consultado agosto 15, 2019. https://play.google.com/store/apps/details?id=com.luizalabs.mlapp&hl=pt_BR

Higa, Paulo. Fim da briga: YouTube volta ao Fire TV e Prime Video estreia no Chromecast. *Tecnoblog*, 2019. Consultado agosto 15, 2019. https://tecnoblog.net/297901/youtube-volta-fire-tv-prime-video-chromecast/

iFood. Cidades Atendidas. *iFood*, s.a. Consultado agosto 15, 2019. https://www.iFood.com.br/cidades-atendidas

iFood. Termos de Uso. *iFood* 2013. Consultado agosto 15, 2019. https://www.iFood.com.br/termos

iFood. Política de Privacidade. Consultado en agosto 15, 2019. https://www.iFood.com.br/privacidade

Jesus, Aline. Magazine Luiza lança F-commerce no Facebook e Orkut. *Techtudo*, 2012. Consultado agosto 15, 2019. https://www.techtudo.com.br/noticias/noticia/2012/02/magazine-luiza-faz-sucesso-com-seu-f-co mmerce-no-facebook-e-orkut.html

Lei nº 8.078. Dispõe sobre a proteção do consumidor e dá outras providências. Setembro 11 de 1990. Consultado agosto 15, 2019. http://www.planalto.gov.br/ccivil_03/leis/l8078.htm

Lei 12.965. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Abril 23 de 2014. Consultado agosto 15, 2019. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Lei 13.709. Lei Geral de Proteção de Dados Pessoais (LGPD). Agosto 14 de 2018. Consultado agosto 15, 2019. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Lei 13.583. Julho 8 de 2019. Altera a Lei nº 13.709, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Agosto 14 de 2018. Consultado agosto 15, 2019. http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm

Letieri. Usuários colocam iFood no sobrenome e não conseguem mudar. Techtudo, 2019. Consultado julio 15, 2019. https://www.techtudo.com.br/noticias/2019/05/usuarios-colocam-iFood-como-sobrenome-no-face book-e-nao-conseguem-mudar.ghtml

Lima, Marina. iFood lança chatbot para pedir pizza no Messenger, mas será se funciona? *Novarejo*, 2017. Consultado agosto 15, 2019. https://portalnovarejo.com.br/2017/07/iFood-chatbot-messenger/

Luna, Denise. MP do DF abre inquérito contra Vivo por suspeita de uso de dados pessoais. *O estado de S. Paulo*, 2018. Consultado octubre 8, 2019. https://link.estadao.com.br/noticias/empresas,mp-do-df-abre-inquerito-contra-vivo-por-suspeita-de-uso-de-dados-pessoais,70002253400

LinkedIn. *Head of Subscription Video Analytics, Prime Video US*. Amazon Job post at Linkedin. Consultado julio 15, 2019. https://www.linkedin.com/jobs/view/head-of-subscription-video-analytics-prime-video-us-at-amaz on-1094636760/

Magazine Luiza. Política de Privacidade. *Magazine Luiza*, 2015. Consultado julio 15, 2019. https://www.magazineluiza.com.br/politica/

Magazine Luiza. E-commerce do Magazine Luiza cresce 56% no segundo trimestre Em menos de três anos, faturamento do Marketplace chega a ¼ das vendas digitais. Release. *Magazine Luiza*, 2019. Consultado en julio 15, 2019. https://ri.magazineluiza.com.br/Download/magalurelease2T19—1-?=Iart1882KdnmVEwBwRdE mQ==&idcanal=rqFYRysdRDkTGGc93mpXJg==

Magazine Luiza. Quem Somos. *Magazine Luiza*, 2019. Consultado en julio 15, 2019. https://ri.magazineluiza.com.br/ShowCanal/Quem-Somos?=urUqu4hANldyCLgMRgOsTw==

Manzoni Jr, Ralphe. Como o Magazine Luiza pretende enfrentar a Amazon? *Istoé Dinheiro*. 2017. Consultado julio 15, 2019. https://www.istoedinheiro.com.br/como-o-magazine-luiza-pretende-enfrentar-amazon/

Medida Provisória n. 869. Dezembro 27 de 2018. Altera a Lei nº 13.709, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Agosto 14 de 2018. Consultado agosto 15, 2019. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869impressao.htm

Meio e Mensagem. Amazon Prime Video e Viacom anunciam conteúdo original. *Meio e Mensagem*, 2018. Consultado en julio 26, 2019. https://www.meioemensagem.com.br/home/ultimas-noticias/2018/11/14/viacom-negocia-series- para-amazon-prime-video.html

Ogilvy y Mather Brasil. Missão Digital Magazine Luiza. Consultado julio 15, 2019. 2017. http://www.ogilvy.com.br/cases/missao-digital

Oliveira, Filipe. Hackers aproveitam erro de digitação em campanha do iFood para infectar consumidores com vírus. *Folha de S. Paulo*. 2019. Consultado julio 26, 2019. https://www1.folha.uol.com.br/mercado/2019/03/hackers-aproveitam-erro-de-digitacao-em-campanha-do-iFood-para-infectar-consumidores-com-virus.shtml

Oracle. New Startups Join Oracle Startup Cloud Accelerator to Enhance Cloud Innovation. 2018 Consultado julio 12, 2019. https://www.oracle.com/br/corporate/pressrelease/startup-accelerator-brazil-second-cohort-2018-06-07.html

Orrico, Alexandre. Tem uma galera dando em cima da vendedora virtual da Magazine Luiza. *Buzzfeed*, 2018. Consultado julio 13, 2019. https://www.buzzfeed.com/br/alexandreorrico/vendedora-virtual-da-magazine-luiza

Pegn. (2018). As 100 startups brasileiras para ficar de olho. Revista Pegn, 2018. Consultado julio 13, 2019. https://revistapegn.globo.com/Startups/noticia/2018/04/100-startups-brasileiras-para-ficar-de-olh o.html

Privacy International. State of Privacy Brazil. 2019. Consultado julio 24, 2019. https://privacyinternational.org/state-privacy/42/state-privacy-brazil

Ricciardi, Alex. Como Frederico Trajano está mudando os rumos do Magazine Luiza. *Forbes*, 2016. Consultado julio 25, 2019. https://forbes.uol.com.br/negocios/2016/07/como-frederico-trajano-esta-mudando-os-rumos-do- magazine-luiza/

Salomão, Karin. "Não tiro a barriga do balcão", diz Luiza Helena Trajano. *Exame*, 2017. Consultado julio 14, 2019. https://exame.abril.com.br/negocios/nao-tiro-a-barriga-do-balcao-diz-luiza-helena-trajano/

Soares, Campos Pedor Silveira. Anonimização na Lei Geral de Proteção de Dados requer posição da ANPD. *Conjur*, 2019. Consultado julio 15, 2019. https://www.conjur.com.br/2019-mar-10/pedro-soares-anonimizacao-lei-geral-protecao-dados#_ftn3

Social Miner. Cases de Sucesso. *Social Miner*, s.a. a. Consultado julio 26, 2019. https://socialminer.com/

Social Miner. "O comportamento do consumidor Online em 2018". Social Miner, 2018. Consultado julio 26, 2019. https://conteudo.socialminer.com/relatorio-comportamento-do-consumidor?utm_source=ECBR&utm_medium=artigo&utm_campaign=relatorio-comportamento-do-consumidor-2018

Social Miner. *Política de Privacidade*. Social Miner s.a. Consultado julio 25, 2019. https://socialminer.com/privacidade.html

Social Miner. *Política de Cookie*. Social Miner s.a. d Consultado julio 25, 2019. https://socialminer.com/cookies.html

Social Miner. Sobre Nós Consultado julio 25, 2019. https://socialminer.com/sobre-nos.html

Social Miner. Social Miner no Oracle Startup Cloud Accelerator. Social Miner, 2018. Consultado julio 15, 2019. http://blog.socialminer.com/people-marketing/social-miner-no-oracle-startup-cloud-accelerator/

Souza, B. Como a Social Miner usa inteligência artificial, mas também gente, para inovar no marketing digital. *Projeto Draft*, 2016. Consultado agosto 15, 2019. https://projetodraft.com/como-a-social-miner-usa-inteligencia-artificial-mas-tambem-gente-para-inovar-no-marketing-digital/

Sousa, G. Páginas Falsas da Magalu no Facebook Tentam Roubar Dados. *Adnews*, 2019. Consultado julio 15, 2019. https://adnews.com.br/internet/paginas-falsas-da-magalu-no-facebook-tentam-roubar-dados/

Vivo. Centro de privacidade. Vivo. Consultado agosto 10, 2019. https://www.vivo.com.br/portalweb/appmanager/env/web?_nfls=false&_nfpb=true&_pageLabel= vivoVivoInstPrivacidadePage&WT.ac=portal.amarca.privacidade&#

Vivo. Termos de Uso do Serviço Amazon Prime Video. Vivo, 2018. Consultado julio 10, 2019. http://ws.mobile.terra.com/Descargas/

Storage/000000000/062000/062250/Terms62250_PT_20181008133419.pdf

Vivo. Vivo para su casa. Consultado agosto 10, 2019. https://www.vivoparasuacasa.com.br/amazonprimevideo/?gclid=EAIaIQobChMIlba8weX_4wIVlI Arch3epwrjeaayasaaegkrivd_Bw

Zuini, Priscila. Movile investe R$ 5,5 milhões na iFood. *Exame*, 2013. Consultado julio 14, 2019. https://exame.abril.com.br/pme/movile-invester-5-5-milhoes-na-iFood/

RENDICIÓN DE CUENTAS DE FACEBOOK Y OTROS NEGOCIOS EN CHILE: LA PROTECCIÓN DE DATOS PERSONALES EN LA ERA DIGITAL

*Paloma Herrera**
*Pablo Viollier***

Introducción

El presente informe tiene como objetivo evaluar el nivel de preparación del ordenamiento jurídico chileno para abordar las nuevas dinámicas de la era digital, así como su capacidad para hacer rendir cuentas a las empresas con modelos de negocios basados en datos (en adelante, EMNBD)[1].

Para ello, el informe estará dividido en cinco secciones. En la primera, se seleccionan cuatro EMNBD y se entrega una justificación de los criterios que permitieron elegir a dichas empresas como representantes de cuatro categorías 1) grandes empresas de Internet, 2) empresas intermedias, 3) start-ups y 4) empresas establecidas. Las cuatro empresas que serán evaluadas por este trabajo son Facebook, PedidosYa, AIRA, y Falabella.

En la segunda sección, se realiza una caracterización y evaluación de la forma de operar de las distintas EMNBD seleccionadas. Esta

* Abogada, Universidad de Chile. Ayudante del Centro de Estudios en Derecho Informático, Universidad de Chile.

** Abogado, Universidad de Chile. Analista de políticas públicas de Derechos Digitales y docente de la Universidad Diego Portales.

1 Para efectos de este informe, las EMNBD serán entendidas como aquellas empresas que cuentan con "modelos de negocios que confían en los datos como un recurso clave" (Hartmann, Zaki, Feldmann & Neely, 2014, p. 6).

caracterización se realizará por medio de un estudio de los distintos términos y condiciones de los productos de las empresas seleccionadas y se articulará en cuatro categorías de análisis: 1) fuente de los datos tratados, 2) tratamiento realizado 3) finalidades de tratamiento y 4) relación con Google, Amazon, Facebook, Apple y Microsoft (en adelante, GAFAM)[2].

En la tercera sección, se busca evaluar en nivel de preparación del régimen jurídico de protección de datos personales chileno para abordar las nuevas dinámicas propias de la era digital. En particular, este análisis se dividirá en dos partes. En la primera, se estudiarán aquellas actividades o dinámicas realizadas por las empresas seleccionadas y propias de la era digital que no estén reguladas en la legislación nacional de protección de datos personales, o que estén reguladas de forma inadecuada. En la segunda, se analiza el alcance del ámbito territorial de la aplicación de la normativa de protección de datos personales y su aplicación extraterritorial a las EMNBD objeto de estudio.

Para ello, se analizará el contenido de la Ley N.º 19.628 sobre protección de la vida privada, así como otros cuerpos normativos nacionales que regulen la recolección, procesamiento y almacenamiento de datos personales. Debido a que Chile se encuentra en un proceso de reforma legislativa de su normativa de protección de datos personales, se realizará un contraste entre las normas actualmente vigentes en la Ley N.º 19.628 y aquellas propuestas en el proyecto de ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (2017), actualmente en discusión. Por último, —y cuando resulte pertinente— se utilizará el Reglamento general de protección de datos de la Unión Europea (GDPR por sus siglas en inglés) como referente para evaluar la pertinencia y nivel de protección de las normas en estudio.

La cuarta sección aborda los mecanismos de observancia de la legislación de protección de datos personales. En particular, se busca dilucidar si el procedimiento de *habeas data* contenido en la Ley 19.628 (de carácter judicial) entrega suficientes garantías para el cumplimiento

---

2 Es importante hacer notar que el informe evaluará el modelo de negocio de estas cuatro empresas en particular, por lo que las conclusiones que se puedan alcanzar respecto de ellas no necesariamente son extrapolables a otras empresas que participen del mismo segmento de mercado o tengan un giro de negocios similar.

de la legislación, el ejercicio de los derechos de los titulares y la capacidad del ordenamiento jurídico para hacer rendir cuentas a las EMNBD.

Por último, se entregan recomendaciones preliminares que apuntan a mejorar la capacidad del ordenamiento jurídico chileno para enfrentar el desafío de las nuevas dinámicas propias de la era digital y los negocios basados en el tratamiento de datos personales.

1. Metodología

La metodología utilizada para efectos de elaborar el presente informe se basa en la revisión y análisis de las políticas de privacidad y condiciones de uso publicadas por las EMNBD en sus portales, de acuerdo con lo descrito en el Anexo 1 del presente informe. Además, se complementa la investigación con información obtenida a partir de las declaraciones efectuadas por las EMNBD en los diversos medios de prensa sobre el funcionamiento y metodología de negocio que manejan. El análisis también incluye un estudio de la regulación nacional, en particular de la Ley N.º 19.628 y las propuestas de reformas en trámite, así como lo dispuesto en el GDPR.

Para complementar este análisis, se realizó un grupo focal el día 4 de octubre de 2019. En esta reunión participaron 11 representantes de la industria, la sociedad civil, la comunidad técnica, organismos públicos y estudios jurídicos especializados en la materia. Las acotaciones realizadas por los participantes del grupo focal se transcriben como forma de complemento del análisis del ordenamiento jurídico, para recoger las impresiones de los actores participantes de la discusión sobre la protección de datos en Chile.

2. Selección de las EMNBD

Si bien el almacenamiento sistemático de datos a nivel corporativo y de organismos públicos es una práctica habitual del siglo XXI, la evolución y masificación de las tecnologías de la información y comunicación (TIC) han impactado en el tratamiento y manejo de datos realizados por las EMNBD. La principal característica que comparten todas las EMNBD, sin importar su tamaño, volumen o grado de consolidación en el mercado, consiste en tratar los datos y utilizar la información obtenida de ellos con el objetivo de implementar avances en temas de innovación y generación de nuevos productos. De esta forma, las empresas enfocan

su gestión en cómo utilizar esta información para atraer más clientes y usuarios a sus respectivos negocios (Diaz y Zaki 2015).

En el contexto nacional, un informe elaborado por la International Data Corporation (IDC), predice que el 60 % del gasto en TI por parte de las empresas para el periodo 2019-2020 será invertido en tecnologías como *cloud computing*, *big data*, internet de las cosas (IoT por sus siglas en inglés) e Inteligencia Artificial (IA), con el objetivo de mejorar su productividad y reducir costos (International Data Corporation, 2018). Por su parte, en el ámbito de la IA, un estudio elaborado por Technology Vision 2019 (Accenture Technology Vision 2019, 2019) determinó que el 46 % de los ejecutivos chilenos encuestados dice que su organización ha adoptado IA, mientras que el 29 % afirma lo mismo a nivel global (TrendTic 2019).

Con el objetivo de describir y analizar el panorama de Chile, se han seleccionado cuatro EMNBD, considerando para tales efectos su grado de consolidación en el mercado chileno y clasificándolas en cuatro categorías: i) grandes empresas de internet, ii) empresas intermedias, iii) start-ups, y iv) empresas establecidas.

2.1. Grandes empresas de internet

Para esta categoría, se seleccionó a Facebook Inc. como una de las empresas agrupadas bajo la sigla de GAFAM (Google, Amazon, Facebook, Apple y Microsoft), conocidas por su posición dominante en el mercado de las tecnologías e información. Se seleccionó esta empresa por contar con cerca de 2271 millones de usuarios activos en todo el mundo (We are Social y Hootsuite, 2019) y superar los 13 millones de usuarios en Chile (Montes 2018). Facebook también representa una empresa ideal para el análisis de este informe ya que su modelo de negocio gira entorno a la recolección y procesamiento de datos personales (e incluso sensibles) para perfilar a sus usuarios y poder vender publicidad personalizada a sus clientes.

Para efectos del presente informe se deja constancia de que, si bien Facebook Inc. ofrece una gran variedad de productos y servicios —destacando la red social Instagram y el servicio de mensajería instantánea WhatsApp— limitaremos la descripción y análisis única y exclusivamente a las condiciones de uso y políticas de privacidad correspondientes a la red social Facebook (Facebook s.d. e).

En este contexto, el poder de concentración y la posición dominante en el mercado que tienen estas empresas ha preocupado a diversos sectores de la sociedad. Conocido fue el caso de Cambridge Analytica, de recolección y procesamiento de un alto número de datos personales compartidos mediante la red social Facebook, y donde Facebook terminó suscribiendo un acuerdo con la Comisión Federal de Comercio de Estados Unidos (FTC, por sus siglas en inglés), comprometiéndose al pago de una multa de 5000 millones de dólares como consecuencia de las diversas irregularidades detectadas en su sistema de privacidad (DW 2019)[3].

2.2. Empresas intermedias

En esta categoría, se eligió a la empresa PedidosYa, compañía de *delivery online* con sede central en Uruguay y con presencia en varios países de Latinoamérica. La empresa está presente en Chile desde el año 2010, donde además tiene ubicada una de sus oficinas principales. Para la elección de esta empresa se consultó el ranking elaborado por la empresa de información y mercado de aplicaciones App Annie (2019)[4], considerando para tales efectos las aplicaciones más descargadas en Chile desde la App Store de Apple y Google Play, según el índice correspondiente a los primeros cinco días del mes de junio de 2019[5].

El modelo de negocio en el que basa su funcionamiento este tipo de aplicaciones está fundamentado en el *e-commerce*, el cual permite a los usuarios acceder a diversos productos y servicios ofrecidos por medio de una plataforma virtual. El funcionamiento de este tipo de plataformas se basa en servir como intermediarios entre el consumidor, el restaurante

---

3 Para ver más detalles sobre el acuerdo alcanzado entre Facebook y la FTC puede consultarse el siguiente enlace de la página de Facebook: https://about.fb.com/ltam/news/2019/07/acuerdo-con-ftc-crea-rigurosos-nuevos-estandares-para-proteger-tu-privacidad/

4 Para ver más detalles sobre la plataforma App Annie: puede consultarse en el siguiente enlace: https://www.appannie.com/das-hboard/home/

5 Si bien en el documento inicial de metodología se consideró estudiar los meses de abril, mayo y junio de 2019, App Annie otorgaba acceso gratuito solo a la información recopilada en los últimos 30 días, por lo que para acceder a la información de periodos anteriores se debía efectuar un pago o interconectar las cuentas de usuarios personales de iTunes y Google Play, lo cual se considera un tratamiento excesivo de la información.

y el repartidor del pedido al cobrar a cada participante de la transacción una comisión por el uso de la plataforma[6] y el servicio de intermediación.

En Chile varias son las empresas que otorgan el servicio de *delivery online* de diversos productos y servicios, donde se destacan las del rubro gastronómico como PedidosYa, Rappi, UberEats, entre otras. Sin embargo, PedidosYa, empresa pionera en el país en el otorgamiento de servicios de este rubro, es la que ha alcanzado la mayor expansión y cobertura de servicio en más de 20 ciudades, desde Arica hasta Puerto Montt[7].

Las ventajas que ofrece la intermediación de estas apps a la industria culinaria, según lo señalado en el sitio web es: 1) Acceso a un nuevo canal de ventas, 2) optimización del sistema entrega a domicilio, 3) sin costos fijos —cargos únicamente en razón de pedidos recibidos—, 4) menú *online* personalizado y 5) compromiso empresarial de PedidosYa (s.d.).

A nivel nacional, la utilización de este tipo de aplicaciones también ha incidido en el aumento en la venta de los productos gastronómicos en general. El Departamento de Estudios de la Cámara Nacional de Comercio, Servicios y Turismo (CNC 2019) reveló que las ventas reales de comida rápida a nivel nacional registraron un crecimiento real anual de 5.4 % durante el primer trimestre del 2019, manifestando la influencia del aumento de la utilización de estas *App delivery* en el país.

2.3. Start-ups

Para seleccionar la empresa correspondiente a la categoría de *start-up*, se consideraron aquellas iniciativas del sector económico y sociocultural que hacen un uso intensivo del conocimiento científico y tecnológico que otorga directamente el mundo de internet para efectos de basar su modelo de negocios en datos (Vega y Ramírez 2018), cuyo modelo de negocios resulte innovador y cuya empresa sea de reciente creación. En este contexto, para este ítem se seleccionó a la empresa chilena AIRA (Artificial Intelligence Recruitment Assistant), la cual ofrece un software de inteligencia artificial que recluta, selecciona y valida antecedentes de

6 Actualmente, se encuentra en tramitación en el Congreso un proyecto de modernización tributaria que establece un impuesto a los servicios digitales con lo que, de aprobarse el referido proyecto, los costos de implementación y uso de estas aplicaciones aumentarían. (Chile, Cámara de Diputados, 2018)

7 En la página web de la aplicación (www.pedidosya.cl) se puede ampliar esta información.

postulantes a puestos de trabajo en un breve tiempo mediante la utilización en conjunto del *Big Data* y la inteligencia artificial.

AIRA comenzó sus operaciones en el año 2016 en el país y en la actualidad es utilizado por más de 30 empresas de los sectores financiero, *retail* y construcción. Lo interesante de esta *start-up* y el motivo de su elección es que señala en su sitio web y en diversos medios de comunicación que tiene la capacidad de organizar rankings de hasta mil currículos en segundos, identificando la experiencia profesional de los candidatos por medio del uso de tecnología biométrica para tales efectos[8].

De acuerdo con lo señalado por el CEO de esta *start-up* a la prensa (Nava 2018), AIRA funcionaría de la siguiente manera:

- Clasificación y envío a los perfiles catalogados como aptos para postular a un determinado cargo un set de preguntas previamente elaborados por AIRA. Cuando los postulantes responden estas preguntas, el sistema analiza sus respuestas y vuelve a generar un listado.
- Los postulantes que hayan pasado a la siguiente etapa, de acuerdo con los resultados otorgados por AIRA, pasarán a lo que se denomina "entrevista virtual", clasificándose las emociones y gestos en positivas, negativas o neutrales.

AIRA señala que la efectividad del proceso radica en que el sistema estaría diseñado para no discriminar por sexo o por edad, por lo que el proceso de contratación sería expedito tanto para la empresa como para los postulantes, evitándose la incertidumbre que ocurre en las entrevistas tradicionales.

Esta empresa ha sido reconocida en diversos concursos globales de Estados Unidos, Suiza y Chile, siendo ganadora de las Olimpiadas Nacionales de Innovación y Emprendimiento de Corfo, y elegida dentro del Top 10 de las empresas tecnológicas más innovadoras de Chile por SeedStars World, además de haber sido contactada por la empresa Y Combinator, de Silicon Valley, una aceleradora de *start-ups* de Estados Unidos (Fajardo 2018).

---

8 El uso de tecnología biométrica, en sí misma, implica una serie de riesgos y eventuales vulneraciones a los derechos de las personas. Para un estudio más en detalle, ver Garrido y Backer (2017).

2.4. Empresa establecida

Para la empresa correspondiente a esta categoría, se eligió a Falabella, una empresa cuyas operaciones comenzaron con anterioridad a la promulgación de la Ley N.° 19.628. Falabella[9] es una empresa de comercio al detalle, fundada en el año 1889 en Santiago de Chile y que ha logrado expandir su negocio a otros países de Latinoamérica (Colombia, Perú y México), gracias a que ha logrado mantener un modelo de negocio ágil, con una fuerte inyección de recursos en tecnología e innovación. Ejemplo de lo anterior es la compra por parte del Grupo Falabella del 100 % de la tienda virtual Linio[10], uno de los principales *market place* de la región.

En la actualidad, Falabella es considerada una de las empresas líderes en el rubro del *e-commerce*, ya que supo adaptarse a los nuevos tiempos, cambiando su modelo de negocio sustentado en una economía basada en la eficiencia de escala a una centrada en el cliente y en la personalización de sus productos y servicios. De tal forma, Falabella ha destacado por inyectar grandes cantidades de dinero en inversión de tecnología, centrándose durante el presente año en potenciar su crecimiento mediante la especialización de sus centros logísticos, gracias a la utilización de *Big Data* e IA.

3. Caracterización de la forma de operar de las EMNBD

Para efectos de describir y analizar la forma de operar de las EMNBD en el país, se sistematizó la información obtenida de sus políticas de privacidad en cuatro categorías de análisis: 1) fuentes de datos, 2) tratamientos de datos, 3) finalidades de tratamiento y 4) relación con GAFAM.

3.1. Fuentes de datos

La Ley N.° 19.628, cuando hace alusión al término 'fuente', lo hace solamente para clasificar a los datos personales objeto de tratamiento de acuerdo al carácter público o privado del lugar desde donde fueron recolectados, sin distinguir si la información fue provista por los titulares.

---

9 Para mayor información, consultar la sección de quiénes somos de su página web (Falabella, s.d.)

10 Linio opera en ocho países con presencia relevante en México, Colombia, Perú, Argentina y Chile, además de tener oficinas en Estados Unidos y China (Linio, s.d.).

Sin embargo, para efectos de este apartado, se consideró como 'fuente de dato' aquella que tiene su procedencia en: 1) información proporcionada por el usuario, 2) datos provistos por terceros y 3) aquellos obtenidos por medio de monitoreo como, por ejemplo, el *webtracking*.

3.1.1. Información proporcionada por el usuario

En la etapa de registro, las cuatro EMNBD coinciden en solicitar como información mínima el correo electrónico, la fecha de nacimiento —para efectos de verificar la mayoría de edad para poder utilizar estos servicios— y una clave o contraseña como control de acceso.

Sobre el requerimiento de clave para acceder a los servicios, se debe destacar el caso de Falabella, quien señala en su portal que el registro de una cuenta asociada con una clave es opcional, señala textualmente: "Esa contraseña no es requisito para contratar en este sitio, pero permite un acceso personalizado, confidencial y seguro" (Falabella s.d.a)[11]. Sin embargo, no otorga mayores detalles sobre por qué es más confidencial o segura la navegación o las transacciones efectuadas mediante una cuenta registrada en desmedro de una compra sin registro, toda vez que Falabella debe cumplir con un protocolo seguro de transferencia de hipertexto (HTTPS por sus siglas en inglés). No se explica ni se infiere el porqué de esta aseveración, pudiéndose interpretar como una forma de desincentivo para la elección de compra sin registro.

Por el contrario, tanto AIRA como Facebook y PedidosYa solicitan el registro obligatorio para poder acceder a sus servicios[12]. Sin embargo, solo PedidosYa explicita dicho requerimiento en su política de privacidad: "Nosotros le proveemos con un identificador de usuario y una contraseña la cual lo habilita a usted a ingresar [a] áreas restringidas de nuestro sitio web u otros contenidos o servicios".

Como información adicional y excesiva solicitada en la etapa de registro, se debe señalar que tanto Facebook[13] como Falabella requieren,

---

11 Destacado de los autores. Para mayor información, véase: https://www.falabella.com/falabella-cl/page/comprar-terminos-condiciones?staticPageId=37900007&menu=comprar&srv=c5

12 Vale la pena mencionar que Facebook permite acceder a ciertas entradas de texto, videos e imágenes que los usuarios han hecho públicas, sin necesidad de que el visitante tenga una cuenta.

13 Facebook pide la información de "sexo" del usuario; sin embargo, otorga en el registro la opción de la categoría "género no binario".

al momento de registrarse en el respectivo portal, información sobre el "sexo" de una persona. Se considera excesiva la solicitud de información relacionada con el género, ya que, si se analiza la finalidad en la recolección y tratamiento de estos datos, lo cual no es otra que facilitar el registro en la red social, debiera bastar con los datos relativos para identificar al usuario por medio de un nombre de usuario y un medio de contacto. No existe aquí justificación suficiente de la obligatoriedad del suministro de información relativa a la identificación con un sexo determinado para efectos del registro. Esta situación ignora que en no todos los casos existe identificación con un género, casos en que el proceso de registro supone la solicitud de información considerada como dato sensible según la legislación nacional. Si bien Falabella solicita información sobre el sexo de manera opcional, Facebook[14] señala la obligatoriedad del suministro de información sobre el sexo y la opción de indicar el género, argumentando para tales efectos la personalización en el envío de mensajes (Ella: Salúdala por su cumpleaños, Él: Salúdalo por su cumpleaños), sin otorgar mayores detalles al respecto.

En el caso de AIRA, el sitio se limita a solicitar correo electrónico y contraseña para su acceso. Sin embargo, también da la opción de interconectar las cuentas de Facebook y Google, pero sin otorgar mayor información al respecto. Es más, los únicos términos y condiciones que hacen alusión a la privacidad y protección de datos visibilizados en el portal están dirigidos a los postulantes de los puestos de trabajo, en forma escueta y general:

> PROTECCIÓN DE PRIVACIDAD: Los POSTULANTES que usan los SERVICIOS de AIRA gozan de todos y cada uno de los derechos de privacidad a los que se refiere la Ley 19.628 de Chile sobre Protección de la Vida Privada y Datos de Carácter Personal, y podrán ejercitar especialmente los derechos de acceder, cancelar, modificar y actualizar su información personal, incluyendo su dirección de e-mail, así como a oponerse al tratamiento de la misma, todo ello de conformidad a lo dispuesto en el cuerpo legal citado.

14 Sin perjuicio de que en el caso de Facebook se indica como opcional el registro de la información concerniente al género.

Más allá de los datos necesarios para llevar a cabo el registro, las otras fuentes de datos recolectadas desde el usuario dependerán del tipo de negocio que desarrollen las EMNBD.

De tal forma, las empresas que están enfocadas en la venta directa (Falabella) o como intermediarios (PedidosYa) de productos, recolectan adicionalmente información relacionada con los productos seleccionados en el carro de compras, dirección de despacho, monto y forma de pago. Lo anterior se vislumbra en sus respectivas políticas de privacidad. Mientras Falabella hace referencia indirecta de lo anterior, al definir como dato personal el "nombre, RUT, domicilio, teléfono, correo electrónico, datos de geolocalización, uso y visita del sitio web, historial de navegación, hábitos de compra, entre otros", PedidosYa señala la recolección de información "acerca de sus visitas y uso de este sitio web incluyendo su dirección IP, ubicación geográfica, tipo de navegador, fuente de referencia al sitio, duración de las visitas y número de vistas por página".

Sin embargo, ninguna de ellas hace explícitas dichas fuentes de información. Asimismo, vale decir que, en el caso de Falabella, esta empresa incluso llega a clasificar este tipo de información como dato personal y no como dato sensible, siendo que a la luz de la legislación nacional debiese recibir un estándar mayor de protección por el simple motivo de que esta información da a conocer hábitos personales del usuario por medio del sitio web.

Al contrario de Falabella y PedidosYa, la red social Facebook otorga mayor detalle y transparencia sobre el tratamiento de este tipo de información, al señalar que cuando un usuario efectúa una transacción por medio de su portal, se incluye dentro del tratamiento "información de pago, como el número de tu tarjeta de crédito o débito y otra información sobre la tarjeta; otra información sobre la cuenta y la autenticación; y detalles de facturación, envío y contacto".

En el caso de AIRA, que ofrece servicios de asistencia a sus clientes en el reclutamiento y selección de personal, la política de privacidad no otorga mayores detalles respecto a otras fuentes de información. Sin embargo, al estudiar las diversas secciones del portal de AIRA, se pueden advertir como fuentes adicionales de datos, los obtenidos por medio del currículo de vida presentado por el postulante, la prueba psicométrica y el video-entrevista denominado Emotion Analytics[15].

---

15 Herramienta que mide las emociones que transmite el postulante

Esta información, al tratarse de datos sensibles conforme a la ley, amerita un abordaje explícito por parte de la política de privacidad del portal. En especial, para satisfacer el objetivo de transparentar la actividad de tratamiento: que se ponga de presente la forma de recopilación de dicha información y su almacenamiento, con tal de asegurar que los titulares de los datos personales estén prestando su consentimiento inequívoco para el tratamiento de este tipo de datos.

3.1.2. Datos generados por medio de monitoreo

Después de analizar las cuatro EMNBD, se concluyó que el monitoreo de datos se da principalmente por medio del *webtracking*,[16] con el objeto de perfilar a un usuario y sus patrones de comportamiento.

En el caso de Falabella y PedidosYa, si bien ambas se centran en el comercio electrónico, centrado en diversos rubros (retail y delivery de comida respectivamente), el comportamiento usual de sus usuarios es navegar por las diversas opciones de productos y servicios con el objetivo de satisfacer una necesidad en específico. En ambos casos la información recolectada gira entorno a sus compras, potenciales compras y hábitos de navegación, con el objetivo de poder ofrecer al usuario ofertas personalizadas para inducirlo a consumir determinados productos.

En el caso de Facebook, desde el punto de vista del usuario común, este utiliza la plataforma para fines lúdicos y de interacción social. Por lo tanto, la información recolectada en este ámbito hace referencia a los contactos (amigos) y empresas (páginas) que el usuario sigue y con las

---

mientras responde las preguntas, lo cual incide en la decisión de contratación por parte del empleador. El uso de este tipo de herramientas ha sido un tema controversial y se ha llegado a señalar que mediante ia es imposible identificar emociones a partir de la expresión facial, ya que el comportamiento de una persona varía mucho dependiendo del contexto concreto y sociocultural, así como tampoco es posible evitar el sesgo de discriminación al ser un humano quien parte catalogando las expresiones. Esto, sin perjuicio de los otros peligros para la privacidad y protección de datos personales, si no se tiene claridad respecto a la fuente de datos, la forma de recopilación y almacenamiento de estos (Feldman, Adolphs, Marsella, Martínez & Pollak, 2019).

16 Mecanismo dirigido a la identificación de dispositivos, navegadores y herramientas que utilizan comúnmente los usuarios de internet. Tiene por objeto la obtención y explotación de estos datos para efectos de recoger, clasificar y recopilar la información con el objeto de tener perfectamente perfilado a un usuario y sus patrones de comportamiento.

cuales interactúa en la red social. A partir de la captura de estos datos, se adelanta su análisis y se ponen a disposición de las marcas que quieran anunciarse en la red social, lo que permite la definición de audiencias específicas para la promoción de sus servicios o productos.

Por su parte, AIRA no otorga mayor información sobre este tema, Falabella, PedidosYa y Facebook hacen referencia a los datos que recopilan mediante el monitoreo en sus respectivas políticas de privacidad. Así, Falabella señala en forma general la utilización de *cookies* analíticas "En Falabella usamos *cookies* y tecnologías similares para personalizar y mejorar tu experiencia de cliente y para mostrarte publicidad online relevante", mientras que PedidosYa en su apartado de *cookies* indica con mayor detalle que usan *cookies* analíticas, de sesión y persistentes al señalar que recopilan "Información acerca de su computadora, y acerca de sus visitas y uso de este sitio web incluyendo su dirección IP, ubicación geográfica, tipo de navegador, fuente de referencia al sitio, duración de las visitas y número de vistas por página".

En cuanto a Facebook, es la que describe con mayor detalle los métodos de monitoreo que emplea. Categoriza los datos obtenidos en razón de los mecanismos utilizados: 1) atributos de dispositivos, 2) operaciones de dispositivos, 3) identificadores, 4) señales del dispositivo, 5) datos de configuración de dispositivos, 6) red y conexiones y 5) datos *cookies* (Facebook s.d.).

3.1.3. Datos proporcionados por terceros

Para la descripción de este apartado, se considerarán aquellos datos que fueron obtenidos por medio de socios estratégicos o terceros. En este caso, solo Facebook indica en sus políticas de privacidad y condiciones de uso los datos proporcionados por terceros en los siguientes términos:

> También recibimos y analizamos contenido, comunicaciones e información que nos proporcionan otras personas al usar nuestros Productos. Esto puede incluir información sobre ti, como en el caso de que otras personas compartan o comenten una foto tuya, te envíen un mensaje o suban, sincronicen o importen tu información de contacto (Facebook s.d. a).

Así como de la información otorgada por sus denominados 'socios'.

> Los anunciantes, los desarrolladores de apps y los editores pueden enviarnos información por medio de las herramientas

> empresariales de Facebook que usan, incluidos nuestros plugins sociales (como el botón "Me gusta"), el inicio de sesión con Facebook, nuestras API y SDK, o el píxel de Facebook. Estos socios nos brindan información sobre las actividades que realizas fuera de Facebook, incluidos datos sobre el dispositivo que utilizas, los sitios web que visitas, las compras que haces, los anuncios que ves y la manera en la que usas sus servicios, ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella (Facebook s.d. a).

Sin embargo, es destacable que Facebook indique que para que terceros faciliten la información exigen que todos los terceros cuenten con derechos legítimos para recopilar, usar y compartir tus datos (Facebook s.d. a). En contraste, AIRA no informa en su política y condiciones sobre los datos que recopila por medio de terceros, lo cual es preocupante, toda vez que su modelo de negocio se basa en los datos que le deben proporcionar las empresas que contratan sus servicios para llevar a cabo el proceso de selección de personal.

3.2. Tratamientos de datos

La Ley N.° 19.628 define como 'tratamiento de datos' cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos de cualquier otra forma. Como es posible apreciar, la legislación chilena establece una definición sumamente amplia de tratamiento de datos, bajo la cual puede entenderse subsumida prácticamente cualquier actividad relevante sobre un dato personal.

Para efectos de la presente investigación, se limitará el estudio a dos de los elementos esenciales reconocidos en la definición legal anteriormente señalada en el contexto de las EMNBD analizadas: 1) recolección y 2) análisis de los datos.

3.2.1. Recolección

La tecnología por excelencia utilizada por las EMNBD para la recolección de datos es mediante el *web tracking* y en específico por medio de *cookies*, como se señaló en el acápite anterior.

Facebook, Falabella y PedidosYa manifiestan en sus respectivas políticas y condiciones la utilización de *cookies*; sin embargo, varían en la especificidad y nivel de información que otorgan al respecto.

En el caso de Falabella, efectúa una referencia genérica sobre el uso de *cookies* de tipo analíticas y señala la utilización de tecnologías similares para personalizar la publicidad y servicios que visualiza un determinado usuario. Sin embargo, no da mayores detalles sobre qué se entiende por 'tecnología similar'. Por el contrario, PedidosYa se destaca por hacer especial énfasis en el tipo de *cookies* que utiliza, explicitando para tales efectos, la utilización de *cookies* de sesión y persistentes, en el siguiente sentido:

> Usaremos *cookies* persistentes para habilitar a nuestro sitio web que lo reconozca a usted cuando visita nuestro sitio. Las *cookies* de sesión serán eliminadas de su computadora cuando usted cierra el navegador web. Las *cookies* persistentes se mantendrán almacenadas en su computadora hasta que sean eliminadas, o hasta que lleguen a una fecha de expiración especificada. (Pedidos Ya s.d. a)

En el caso de Facebook, como se señaló anteriormente, cuenta con una política especial dedicada a las *cookies*, al igual que Falabella que hace alusión al uso de "otras tecnologías" sin otorgar mayores detalles al respecto, señalando que para efectos de aquella política, serán consideradas como "*cookies*" sin explicitar los límites y alcances de estas aseveraciones.

Si bien Facebook, a diferencia de PedidosYa, no clasifica el tipo de *cookies* que maneja, sí realiza una descripción detallada al ejemplificar su funcionamiento. En este sentido, Facebook, sin señalar textualmente al momento de hacer referencia a las *cookies* de personalización para fines publicitarios, otorga el siguiente ejemplo:

> Utilizamos *cookies* para contar el número de veces que se muestra un anuncio y calcular su costo. También utilizamos *cookies* para medir la frecuencia con la que se realizan determinadas acciones, como hacer clic en un anuncio o verlo[17].

---

17 Asimismo, Facebook cuenta con sitios específicos sobre cada tipo de cookie (https://www.facebook.com/policy/cookies?list) y una política general de cookies (https://www.facebook.com/policy/cookies)

Por su parte, AIRA no hace mención a las *cookies* ni a la utilización de otras tecnologías para la recolección de información. Sin embargo, se encontró que, al momento de analizar el código fuente de todos los sitios web asociados con las EMNBD, el sitio de AIRA y el de PedidosYa —que otorga información de las *cookies* que utiliza desde la categoría de duración de las *cookies*—, utilizan la herramienta Hotjar, cuyo uso lamentablemente no se especifica en ninguna de las políticas de estos sitios.

Hotjar es una suite de análisis de datos utilizada en el contexto de marketing digital, la cual combina en una sola plataforma varias funcionalidades de recopilación y análisis de datos. En este contexto, llama la atención que dentro de sus principales funcionalidades indica la elaboración de 'mapas de calor' (registra dónde hacen clic los usuarios de un sitio web) y la posibilidad de grabar las sesiones de los usuarios en el sitio web (monitoreo de las grabaciones de los usuarios para observar lo que están haciendo exactamente).

El uso de Hotjar es un claro ejemplo de cómo se utilizan las *cookies* para fines publicitarios y de cómo se almacenan datos sobre hábitos de navegación, por lo que la omisión en las políticas de privacidad de esta información puede vulnerar la expectativa de privacidad[18] de los usuarios al momento de navegar en los portales de las EMNBD. En el caso de PedidosYa, si bien omite mencionar el uso de Hotjar, es la única en señalar explícitamente en sus términos y condiciones la utilización de Google Analytics para la generación de información estadística sobre el uso del sitio a través de *cookies*.

Facebook, por su parte, si bien no menciona los algoritmos ni herramientas analíticas que utiliza, hace alusión a la colaboración que esta hace con ciertos proveedores de datos como como Acxiom, Oracle Data Cloud (antes DLX), Epsilon, Experian y Quantium, donde el tercero que utiliza los servicios de estos proveedores de datos proporciona dicha información a Facebook[19].

---

18 Concepto desarrollado en EE.UU. UTILIZADO POR LA JURISPRUDENCIA NORTEAMERICANA CON LA FINALIDAD DE EVALUAR LOS LÍMITES DE LA PRIVACIDAD EN CADA CASO EN CONCRETO (SALDAÑA, 2001).

19 Según un reciente anuncio de Facebook, el acceso a cierta información por terceras partes se verá limitado a propósito del arreglo que alcanzó con la FTC estadounidense (Facebook, 2019).

3.2.2. Análisis

En el ámbito de las EMNBD, estas recolectan datos con el objetivo de procesarlos y canalizarlos para la generación de información de gran valor corporativo, para efectos de identificar patrones de consumo o estrategias óptimas de fidelización de clientes. Lo anterior permite a las empresas satisfacer las necesidades del usuario y elaborar una estrategia de negocio para optimizar los servicios en función del comportamiento del usuario.

En cuanto al análisis, el mismo es normalmente de tipo descriptivo, encaminado a segmentar a los usuarios y a las audiencias de acuerdo con sus habilidades, gustos, intereses y conexiones, o prescriptivo, entendiéndose este concepto como lo que debiera suceder para mejorar la experiencia del usuario en futuras visitas.

Desde el ámbito descriptivo, tanto Falabella como Facebook señalan en sus políticas de privacidad que efectúan análisis de datos con el objeto de segmentar a sus usuarios para la personalización del contenido y/o productos que se ofrecen. Así, Facebook señala en resumen que lo realiza para sugerir comunicaciones con otros usuarios, páginas al interior de Facebook y anuncios relevantes, dependiendo de la ubicación otorgada por el GPS. Mientras que Falabella señala que lo hace para preparar, promocionar y ofrecer nuevos productos y servicios y además para efectos de que el usuario pueda participar de los beneficios del programa de fidelización de CMR PUNTOS (Falabella s.d. a).

En el caso de AIRA, no obstante lo escueto de sus políticas de privacidad, la información otorgada por los postulantes a los puestos de trabajo requeridos por las empresas que contratan con los servicios de AIRA es estandarizada y clasificada de acuerdo con los requerimientos de las empresas. Al respecto, AIRA (2019) señala:

> Responsabilidad de AIRA: a) Suministrar SERVICIOS en forma correcta, oportuna y cabal, tal que todos los POSTULANTES estarán sujetos a procesos de selección definidos por la EMPRESA, pero ejecutados por la tecnología de AIRA de forma objetiva y estandarizada, dando así oportunidades iguales a todos los POSTULANTES para brindar y convencer a la EMPRESA de su afinidad con la oferta laboral.

Por su parte, PedidosYa (s.a.), no hace referencia sobre este tema limitándose a señalar:

> Cualquier usuario podrá hacer uso del servicio PedidosYa, siempre y cuando esté comprendido dentro de los siguientes grupos definidos: Usuario anónimo: Cualquier usuario de internet. Usuario registrado: Cualquier usuario que fuera previamente registrado gratuitamente en el sitio de datos básicos.

En cuanto al análisis prescriptivo, el cual tiene por objeto mejorar la experiencia del usuario, las EMNBD se limitan a señalar las finalidades del tratamiento para efectos de lograr este objetivo más que otorgar mayor información sobre describir las herramientas y sistemas automatizados utilizados para efectuar sus análisis.

3.3. Finalidades del tratamiento

El principio de finalidad es considerado el pilar rector de toda normativa que regule el tratamiento de datos personales. No basta con que la recolección de los datos cumpla con los estándares legales, su utilización debe responder a la finalidad para la cual fueron recolectados. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga conforme a la ley y para las finalidades permitidas. Si los datos son tratados para fines distintos a los consentidos por el titular o no autorizados por la ley, el tratamiento de dichos datos es ilegítimo.

Las motivaciones que tienen las EMNBD para recopilar datos personales son diversas: otorgar el servicio, crear perfiles de usuarios y analizar el comportamiento del consumidor. Todas estas finalidades deben ser informadas y consentidas por el usuario de forma anterior a la recolección y procesamiento.

De acuerdo con lo anterior, se clasificaron las finalidades en tres categorías: 1) para el uso de los productos, 2) personalización de contenidos y 3) envío de comunicaciones al usuario.

AIRA hace una referencia genérica a las finalidades de su tratamiento, al señalar: "AIRA solo podrá utilizar la INFORMACIÓN propietaria [sic] del POSTULANTE con relación a los SERVICIOS materia de estas CONDICIONES", detallando como finalidad la entrega de la información personal recopilada y analizada a la Empresa que contrató los servicios IA ofrecidos por AIRA para efectos de llevar a cabo la selección de personal.

En el caso de Falabella y PedidosYa, se destaca el hecho de otorgar información sobre las finalidades del tratamiento de datos, por medio de un listado de fácil entendimiento para el usuario. Así, Falabella indica

que además sus empresas relacionadas, podrán tratar los datos personales en general para la personalización del contenido y para la venta de sus productos y servicios al cliente/usuario:

> Tus datos personales podrán ser tratados por Falabella y/o sus Empresas Relacionadas, por sí o a través de sus proveedores, exclusivamente para (i) preparar, implementar, promocionar y ofrecerte nuevos productos y servicios, o bien, nuevos atributos, modalidades o características a los productos y servicios que ya están a tu disposición; (ii) completar automáticamente los documentos asociados a las transacciones que realices en función de los productos adquiridos y/o servicios utilizados o contratados, o que en el futuro adquieras, utilices o contrates, con Falabella o sus Empresas Relacionadas; (iii) acceder a, procesar y tratar tu información, a fin de ajustar la oferta de productos y servicios a tu perfil de cliente, o bien, efectuar análisis, reportes y evaluaciones a su respecto; y (iv) desarrollar acciones comerciales o servicios de post venta, de carácter general o dirigidas personalmente a ti, tendientes a mejorar tu experiencia como cliente.

Por otro lado, PedidosYa señala que podrá utilizar información personal para:

> i) administrar el sitio web, ii) mejorar la experiencia de navegación personalizada del sitio web, iii) Habilitar al usuario para el uso de los servicios disponibles en el sitio web, iii) Enviar comunicaciones comerciales generales, iv) Enviar notificaciones por email solicitadas por usted específicamente y v) Enviarle nuestra newsletter y otros comunicados relacionados con el sitio web que creemos que será de su interés, donde usted aceptó específicamente esto, por email.

Sin embargo, sobre este último punto, se debe señalar que PedidosYa tiene seleccionada por defecto la casilla donde el usuario autoriza recibir publicidad y otro tipo de información. Lo anterior es lamentable, toda vez que es de público y lato conocimiento que los usuarios no leen las condiciones de uso ni las políticas de privacidad y aceptan rápidamente todos los términos y condiciones para efectos de poder utilizar los servicios, autorizando en consecuencia múltiples tratamientos para finalidades publicitarias e ignoradas por el titular de los datos. Si bien no

corresponde catalogar esta conducta como ilegal, sí constituye una mala práctica, ya que existe consenso en la doctrina que el consentimiento del titular siempre debe ser informado, expreso y específico.

Para finalizar, en el caso de Facebook, la red social señala de forma general "debemos tratar tu información a fin de proporcionarte los productos de Facebook", no otorgando un listado claro de finalidades y de fácil acceso al usuario. En efecto, solo el usuario que pueda invertir el tiempo suficiente en leer de los diversos documentos que componen las políticas y condiciones generales de uso de Facebook podrán entender estas finalidades, las cuales están disgregadas en todo el portal de la red social[20].

3.4. Relación con las GAFAM

Todas las empresas que basan sus negocios en modelos de datos, de una u otra forma se relacionan con Google, Amazon, Facebook, Apple o Microsoft. En específico, de las cuatro EMNBD, y considerando el caso específico de Facebook y su relación con AIRA, PedidosYa y Falabella; estas interactúan, por una parte, por medio de las páginas que Facebook ofrece a las empresas para fines publicitarios (Facebook 2014) y, por otra, desde la interoperabilidad de sus plataformas (mediciones, análisis y otros servicios empresariales).

Sobre la presencia de las empresas por medio de la creación de páginas de Facebook, tanto Falabella, AIRA y PedidosYa tienen páginas oficiales en Facebook para efectos de generar publicidad, ser un canal de comunicación directo con sus usuarios y generar anuncios al interior del sitio (Facebook s.d. d).

En cuanto a la interoperabilidad de Facebook con las demás empresas, lo cual debe ser entendido como la capacidad que tiene un sistema para funcionar y relacionarse con otros sistemas existentes, se debe hacer especial mención al caso de PedidosYa, ya que otorga la posibilidad de

---

20 A modo de ejemplo, al momento de hacer referencia a la fuente de recopilación de datos, en el apartado de recopilación de datos biométricos mediante cámara, Facebook señala que esta tiene solo por finalidad la de "realizar acciones como sugerirte máscaras y filtros que quizá te gusten, así como darte consejos sobre cómo usar los formatos de cámara", sin embargo, en otro apartado se señalan otras finalidades donde se infiere que podrían utilizar los datos recopilados, ya sea para fines de investigación o publicitarios, por decir algunos ejemplos.

efectuar un registro rápido mediante la interconexión con la cuenta de Facebook[21].

Cuando el potencial usuario de PedidosYa decide elegir esta forma de registro, otorga automáticamente a la empresa acceso a la información almacenada en Facebook, lo cual puede llegar a ser considerado un tanto excesivo, si se consideran las motivaciones del usuario —registro rápido en el sitio— y las finalidades de PedidosYa para el tratamiento de estos datos (la entrega a domicilio de productos comercializados por terceros). Lo anterior se verifica al momento de consultar la sección de Facebook correspondiente a "Cómo PedidosYa puede usar tu información", donde simplemente se limita al señalar que "PedidosYa puede usar la información que proporcionas para personalizar tu experiencia y conectarte con tus amigos".

Esto último resulta preocupante y contrario al principio de finalidad, ya que, si se relaciona con los términos y condiciones de Facebook, ellos señalan que al momento de vincular una aplicación (e.g. PedidosYa) con una cuenta de Facebook, se está otorgando permiso a la aplicación para acceder información contenida en Facebook, tal como la edad, el idioma de uso, el sexo, e incluso la lista de amigos, quienes son terceros que no han otorgado explícitamente su consentimiento. En razón de lo anterior, PedidosYa debería transparentar en su respectiva política los límites y consecuencias de efectuar un registro mediante la interconexión de las cuentas, ya sea explicitando en su portal o remitiendo al usuario al apartado específico de Facebook donde se señalan las condiciones de uso de este tipo de datos.

4. Nivel de preparación del régimen jurídico de protección de datos personales

La Ley N.º 19.628 sobre protección de la vida privada fue promulgada el 18 de agosto de 1999, siendo una de las primeras legislaciones que regula

---

21 Al respecto, vale la pena mencionar que recientemente Facebook anunció la creación de "Off Facebook Activity", una plataforma al interior de Facebook que permite al usuario ver y controlar los datos que las aplicaciones y sitios web comparten con Facebook. Sin embargo, al momento de la redacción de este informe, esta plataforma aún no se había implementado para los usuarios de América Latina (Facebook, 2019).

la protección de los datos personales en la región. Sin embargo, incluso desde antes de su publicación, el cuerpo legal fue descrito como insuficiente para proteger a los titulares de datos personales del tratamiento realizado por parte de terceros (Jijena 2001).

Hoy existe un consenso entre los expertos, la academia y la sociedad civil en torno a la falta de adecuación de la ley para una efectiva protección de los datos personales (Comité Evaluación de la Ley 2016). Este deficiente nivel de protección no solo se explica por el transcurso de los años, sino también porque su elaboración estuvo fuertemente influenciada por intereses particulares. El proceso de su discusión legislativa estuvo marcado por una importante participación e incidencia de los representantes de industrias interesadas en la explotación de datos personales, en desmedro de la influencia ejercida por la academia y la sociedad civil. En palabras de Jijena (2010), la Ley N.º 19.628 fue redactada "con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento de los parlamentarios que la impulsaron". De esta forma, es posible aseverar que el objetivo de la ley fue ofrecer un marco regulatorio para el mercado de las bases de datos, antes que generar un sistema que buscara proteger la autonomía informativa y los derechos de los titulares desde una perspectiva de derechos fundamentales.

Entre las principales falencias de la legislación actual se pueden mencionar:

> [...] la ausencia de sanciones efectivas, la falta de regulación del flujo transfronterizo de datos personales, la autorización del uso de datos para marketing directo sin consentimiento del titular, la falta de registro de bancos de datos privados, la ausencia de una autoridad pública de control, excepciones amplias al consentimiento para el tratamiento de datos, y la falta de mecanismos procedimentales de resguardo efectivo (Derechos Digitales, 2017, p. 4).

El impulso para modificar y actualizar la normativa chilena de datos personales ha estado determinado por dos factores. El primero, es el compromiso adquirido por Chile ante la Organización para la Cooperación y el Desarrollo Económicos (OCDE), al momento de ingresar a dicha instancia internacional, consistente en implementar las Directrices relativas a la protección de la privacidad y el flujo transfronterizo de

datos personales (OCDE 2002) y, en menor medida, por compromisos relativos al derecho a la privacidad y tráfico transfronterizo del Foro de Cooperación Económica Asia-Pacífico (APEC, por su sigla en inglés), aunque estos establecen un esquema de protección menos robusto que las directrices de la OCDE (APEC 2005; APEC 2009). El segundo, es el anhelo por parte de Chile de elevar su nivel de protección y alcanzar el estatus de legislación adecuada de acuerdo con los estándares establecidos en el Reglamento general de protección de datos de la Unión Europea.

Chile ha emprendido dos importantes procesos de reforma. El primero, fue la modificación del Artículo 19, número 4 de la Constitución, que elevó la protección de datos personales a nivel constitucional. El numeral cuarto hoy establece que:

> La Constitución asegura a todas las personas [...] 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley.

El segundo, es el Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, presentado el 15 de marzo de 2017 con el objetivo de elevar el estándar de protección de datos personales y cumplir con las exigencias de la OCDE en la materia.

En las siguientes secciones se analizarán aquellos aspectos de la legislación vigente que no regulan o que regulen de forma deficiente aquellas actividades propias de la era digital y que realizan las EMNDB estudiadas en la sección anterior.

4.1. Carencias regulatorias

4.1.1. Datos sensibles inferidos y los datos de los que se infieren

La Ley N.° 19.628 define los datos sensibles en su Artículo 2, literal g, como:

> [...] aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las

creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

La legislación define la categoría de dato personal sensible sin distinguir la forma en que estos datos son obtenidos. En este sentido, una interpretación sistemática de la legislación permite concluir que el responsable de base de datos debe cumplir con los requisitos adicionales que la categoría dato personal sensible conlleva, independiente de si el dato es obtenido por medio del consentimiento del titular o por medio de un tratamiento automatizado que permite inferir un dato sensible.

Esto es particularmente relevante respecto del modelo de negocio de algunas de las EMNBD estudiadas, ya que son justamente los datos inferidos los que permiten perfilar a los usuarios, ya sea para conocer su historial de compras y ofrecerles productos personalizados o para conocer sus hábitos personales y entregarles publicidad dirigida.

Esta interpretación cobra sentido al tener en consideración la naturaleza jurídica del vínculo entre el titular y sus datos personales. Esta relación de titularidad, en oposición a otras formas de vínculo jurídico como el dominio o la propiedad, implica que el titular no puede renunciar, ceder o enajenar su capacidad de control sobre los datos relativos a su persona (Contreras 2019). En el mismo sentido, los titulares se encuentran habilitados para ejercer su derecho de acceso, rectificación, cancelación u oposición de sus datos personales, incluso si ellos han sido inferidos por el responsable de base de datos mediante mecanismos algorítmicos o automatizados. Lamentablemente, en Chile no ha existido jurisprudencia que se pronuncie sobre este punto en específico, dejándolo relativamente abierto a la interpretación y generando incertidumbre jurídica para los derechos de las personas.

El Proyecto de Ley de datos personales no menciona los datos inferidos en ninguno de sus artículos. El Artículo 9º del Boletín Nº 11.144-07 regula el derecho a la portabilidad de datos personales, estableciendo que los responsables de bases de datos están obligados a entregar una copia, de manera estructurada, de los datos personales que conciernen a los titulares, en un formato genérico y de uso común, que permita ser operado por distintos sistemas cuando estos así lo soliciten.

No obstante, la letra a) del Artículo 9º del proyecto señala que "[n]o procede el ejercicio de este derecho respecto de la información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamientos

realizados por el responsable". La justificación de este apartado se encontraría en el hecho de que permitir la portabilidad de datos inferidos generaría un problema en el mercado del tratamiento de datos personales, permitiendo a cualquier competidor acceder a información que fue generada o inferida por medio de mecanismos de carácter privado, protegido por secretos industriales o derechos de autor. Sin embargo, la limitación sobre los datos inferidos solo alcanza al ejercicio del derecho a portabilidad, y por tanto los titulares de datos personales se encontrarían plenamente habilitados para ejercer todos los derechos que les concede la legislación sobre los datos inferidos, incluido el derecho de acceso, debiendo el tratamiento de este tipo de datos cumplir con los mismos requisitos que un dato obtenido por medio de otros mecanismos que habilitan el tratamiento de datos personales y datos personales sensibles.

Por último, el hecho de que la definición vigente de datos sensibles incluya entre sus ejemplos los hábitos personales, entrega elementos interpretativos para concluir que el comportamiento, la rutina y otros aspectos de la vida íntima de los titulares se encuentran expresamente protegidos por la legislación. En este sentido, el perfilamiento de los usuarios y sus hábitos personales muchas veces se realiza por medio de datos que son inferidos a partir de antecedentes como su historial de compra, navegación o localización, información que se encontraría dentro de la actual definición de dato personal sensible. Esta discusión es relevante porque durante la tramitación del proyecto de ley en la Comisión de Constitución del Senado se decidió eliminar del proyecto original una mención expresa a los hábitos personales como dato personal sensible, lo que constituye un evidente retroceso respecto al estándar actual de protección (CIPER 2019).

En consecuencia, surge una importante discusión respecto a la legalidad del uso de *cookies* por parte de las empresas estudiadas. Si los hábitos personales (entre los cuales se puede considerar a la navegación web) son datos de carácter sensible, entonces se requiere un consentimiento expreso del titular para su tratamiento[22]. Sin embargo,

---

22 El artículo 10 de la Ley N.° 19.628 establece un catálogo taxativo de situaciones en las cuales un tercero estará habilitado para tratar datos sensibles del titular: 1) contando con el consentimiento del titular, 2) estando autorizado por ley y 3) sean se trate de datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

resulta discutible que la inclusión del uso de *cookies* entre los términos y condiciones aceptadas por el usuario cumpla con el requisito de que el consentimiento sea expreso, informado y específico.

Por otro lado, el hecho de que la definición amplia de datos personales contenida en la legislación chilena permita al titular retener el control sobre los datos que plataformas como Facebook infieren respecto de él, abre una importante discusión: la posibilidad de los titulares de ejercer sus derechos ARCO respecto de esta evaluación poco transparente que la plataforma realiza a partir de su comportamiento en línea. Por ejemplo, si la plataforma procesa los datos de un usuario y los clasifica como una persona de opiniones políticas conservadoras, esta información debe considerarse de carácter sensible, por tener relación con la inclinación política del titular. De esta forma, sería necesario permitir al titular un mecanismo para obtener acceso a esta evaluación y rectificarla si esta es incorrecta, desactualizada o imprecisa.

Al respecto, un participante del grupo focal perteneciente al sector industria señaló que le parecía importante que "las definiciones sean lo más amplias y flexibles posibles" y que la definición "de dato sensible está bien que sea un catálogo, pero no debería ser estricto". En un sentido similar, otro experto en la materia acotó que "lo importante es que las definiciones se puedan adaptar. Interpretar es tarea de la autoridad y los tribunales a la luz de las nuevas tecnologías y formas de tratamiento".

Sobre el estatus jurídico del dato inferido, un representante de un organismo público, cuya labor se relaciona con la protección de datos personales, mostró una posición similar a la presentada en este informe, al señalar que:

> [...] el dato inferido es problemático, también hay datos observados y datos personales. La respuesta no es simple, no está resuelta en Europa. Nosotros tenemos la ventaja que tenemos el hábito personal como dato sensible y eso se puede aplicar al dato inferido. Uno puede decir que el dato inferido es una opinión o una consecuencia de un análisis jurídico (es probabilístico).

4.1.2. Los protocolos de internet (IP) e identificadores similares, y los datos asociados con ellos

El Artículo 2º letra f) de la Ley N.º 19.628 define los datos de carácter personal o datos personales como aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables".

Esta definición es relevante, puesto que establece el ámbito de aplicación de la ley: esta solo es aplicable al tratamiento de información personal.

Para efectos de este análisis, resulta relevante la posibilidad de que un dato pueda ser considerado de carácter personal por referirse o estar vinculado con una persona determinable. De acuerdo con Cerda (2012, 16), un dato podrá ser considerado personal cuando permite identificar a una persona utilizando "el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona". De esta forma, a pesar de que la legislación no se refiere específicamente a la dirección IP como dato personal, sería posible interpretar que esta corresponde a un dato personal en la medida de que vaya acompañada de otros antecedentes que permitan la identificación de una persona determinada (datos de geolocalización, *webtracking*, entre otros).

Por otro lado, el único cuerpo jurídico que se refiere específicamente a la dirección IP es el Artículo 222, inciso quinto, del Código Procesal Penal, que establece la obligación de que las empresas de telecomunicaciones mantengan "en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados". Se trata, por lo tanto, de un esquema de retención general de metadatos cuya constitucionalidad es dudosa, en atención a la desproporción de la medida y la afectación del derecho a la intimidad de la población (Canales y Viollier 2018).

Por tanto, este es un caso límite en donde lo que corresponde dilucidar es si la dirección IP en un caso permite que esta se vincule con una persona determinada. La Corte Suprema de Chile se ha referido a la posibilidad de que un dato sea de carácter personal, al permitir que este sea asociado con una persona determinada. De esta forma, sentenció que las placas patentes vehiculares pueden ser consideradas como datos personales, en la sentencia de la causa Rol N.º 2479-2018, donde la Corte sostuvo que un reportaje que fue objeto de acción judicial:

> [...] incluyó la imagen de un vehículo marca Audi, sin borrar ni distorsionar la parte del cuadro que mostraba dicha placa y permitía, por ende, a cualquier persona que viera el programa identificar con un mínimo esfuerzo de búsqueda quién es el propietario del vehículo y, eventualmente, relacionarlo con el contenido del reportaje.

De esta forma, la Corte parece establecer un test del mínimo esfuerzo de búsqueda. En contraste, el Reglamento General de Protección de Datos de la Unión Europea establece en su artículo 26 que "[p]ara determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física".

Un criterio similar ha tenido el Consejo para la Transparencia en la causa C-611-2010, en donde se pronunció específicamente respecto de la naturaleza del número de teléfono como dato personal, señalando que:

> [...] desde el punto de vista de la protección de los datos personales, en tanto el número de teléfono se encuentre asociado o sea susceptible de asociarse al nombre de una persona natural, dicha información constituye un dato personal, por lo que quienes trabajen en su tratamiento están obligados a guardar secreto sobre los mismos, cuando estos provengan o hayan sido recolectados de fuentes no accesibles al público.

El hecho de que un dato pueda ser considerado de carácter personal, si mediante un mínimo esfuerzo puede vincularse con una persona determinada, también ha permitido argumentar que el número de teléfono móvil —en el marco de una solicitud masiva de información por parte del regulador a las empresas de telecomunicaciones— puede ser considerado como un dato personal, si va acompañado de otros datos que permiten perfilar al cliente (Canales 2019). Un razonamiento similar ha sido utilizado por el derecho europeo para considerar la dirección IP de un dispositivo y la dirección de casilla de correo electrónico (incluso cuando esta no coincida con el nombre de su titular) como un dato personal[23].

En síntesis, existen suficientes antecedentes en la legislación y la jurisprudencia chilenas para argumentar que la dirección IP puede ser considerada un dato personal, si por medio de otros antecedentes puede vincularse con una persona determinada. Sin embargo, es deseable que la legislación ofrezca pautas claras para interpretar este caso específico. Por ello, resulta preocupante que el proyecto de ley no se pronuncie específicamente sobre la dirección IP y en qué casos esta podría ser

---

23 Entre otras, pueden citarse la Sentencia C-582/14 del Tribunal de Justicia de la Unión Europea.

considerada como un dato personal. Sin embargo, el Artículo 2.º, letra f) del proyecto define dato personal como:

> [...] cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información combinada con otros datos, en particular mediante un identificador, tales como el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado" (destacado nuestro).

De esta forma, el hecho de que se incorpore la figura de la información combinada con otros datos entrega herramientas adicionales a la hora de interpretar cuándo un dato puede vincularse a una persona identificable.

Esta mención se encuentra en la sección de considerandos del proyecto, por lo que no constituiría una regla vinculante. Sin embargo, sirve como elemento a tener en consideración al momento de interpretar el alcance de la dirección IP como dato que puede ser considerado personal, si es posible asociarlo con una persona determinada.

Lo anterior es relevante, puesto que el análisis de las empresas realizado en el apartado anterior da cuenta de que el uso de *cookies* permite la recolección de la dirección IP como dato. De las empresas estudiadas, solo PedidosYa menciona expresamente la dirección IP; sin embargo, no es difícil imaginar que las otras empresas que utilizan *cookies* también recolectan este dato. Una investigación más profunda sería necesaria para averiguar qué tipo de uso se le entrega a la dirección IP, si las empresas cruzan dicha información con otros datos que permitan identificar al usuario mediante la IP y si las empresas, considerando la dirección IP como dato personal, en consecuencia toman los resguardos necesarios respecto a su tratamiento o si, por el contrario, consideran de que se trata de información de carácter estadístico.

4.1.3. Perfilamiento

Las cuatro EMNBD estudiadas basan su oferta de valor en el perfilamiento de sus usuarios, ya sea para ofrecerles servicios o productos

personalizados, ofrecer avisaje a segmentos demográficos específicos, o para selección de personal. En efecto, es posible argumentar que el perfilamiento de los usuarios se encuentra en el corazón del modelo de negocios de muchas de los principales gigantes de Internet, entre las que se encuentran las GAFAM. Esto representa un desafío importante en términos regulatorios, toda vez que el perfilamiento tiene el potencial de vulnerar los derechos fundamentales de los titulares, ya sea por la asimetría de poder que crea entre el usuario y la plataforma, el eventual rastreo y monitoreo de actividades requerido para su ejecución y la personalización o manipulación del comportamiento que puede generar (Büchi, Fosch, Lutz, Tamò-Larrieux, Velidi y Viljoen 2019).

La Ley N.º 19.628 no regula explícitamente la creación de perfiles o el perfilamiento de los titulares de datos personales. Sin embargo, el hecho de que los hábitos personales se encuentren definidos como un dato personal sensible, entrega elementos interpretativos para argumentar que los datos obtenidos mediante el proceso de perfilamiento pertenecen a esta categoría y, por tanto, se encontrarán especialmente resguardados. Esto quiere decir que su tratamiento está sujeto a una serie de requisitos adicionales.

Esta es una materia abordada por el proyecto de ley de datos personales hoy en discusión. Una de las indicaciones al proyecto presentadas por el ejecutivo en julio de 2018 modifica el Artículo 2º letra w), que define la creación de perfiles:

> [...] como toda forma de tratamiento automatizado de datos personales que consista en utilizar esos datos para evaluar, analizar o predecir aspectos relativos al rendimiento profesional, situación económica, de salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona natural.

Esta inclusión permite caracterizar de forma más precisa una actividad central del modelo de negocio de muchas plataformas en línea. No obstante, el articulado no otorga al resultado del perfilamiento la categoría de dato personal sensible; por el contrario, en el proyecto esa definición se reduce a:

> [...] aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos

> relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

Del mismo modo, como fue dicho, la eliminación del hábito personal, como dato personal sensible, hace más difícil interpretar que los datos que resulten del perfilamiento gocen del nivel más elevado de protección, por lo que el proyecto de ley corre el riesgo de reducir el nivel de protección que otorga actualmente la legislación vigente (CIPER 2019).

Por su parte, el GDPR define la elaboración de perfiles en su Artículo 4, número 4, como:

> [...] toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

La definición es prácticamente idéntica a la contenida en el proyecto de ley chileno, lo que da cuenta de la influencia de la regulación europea. Del mismo modo, el GDPR menciona la elaboración de perfiles a propósito del derecho a oposición, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado.

4.1.4. Toma de decisiones automatizadas

Al igual que en el caso del perfilamiento, la toma de decisiones automatizadas[24], así como la toma de decisiones determinadas por medios algorítmicos, representan una eventual amenaza para los derechos fundamentales de los titulares (Derechos Digitales 2016).

De acuerdo con boyd y Crawford (2011), existe una tendencia a mostrar los resultados del análisis de datos como un asunto de hechos y no de interpretación, dotando de esta forma a la toma automatizada de decisiones de un manto de objetividad. Sin embargo, la programación

---

24 Para estos efectos, se entiende que la toma automatizada de decisiones puede ser definida como "la habilidad de tomar decisiones por medios tecnológicos sin intervención humana" (Grupo de Trabajo del Artículo 29, 2017, citado en Newman & Arango, 2019, p. 66).

de un mecanismo automatizado o algoritmo requiere de una decisión respecto de qué datos se utilizarán para la toma de decisiones y cuáles son los parámetros que se buscan optimizar, todas las cuales son decisiones humanas sujetas a sesgos propios de sus programadores (Malik 2019). De esta forma, es posible que un mecanismo automatizado llegue a resultados discriminatorios o arbitrarios con base en información objetiva. Por otro lado, la complejidad técnica de estos mecanismos, sumado al hecho de que estos algoritmos muchas veces están protegidos por secretos industriales y otras figuras de propiedad intelectual, pueden generar una capa de opacidad respecto de cómo se toman las decisiones. Lo anterior explica la tendencia en la legislación comparada reciente de incluir herramientas para promover la transparencia algorítmica, así como el establecimiento de reglas que buscan proteger a las personas de este tipo de toma de decisiones cuando estas pueden provocarles efectos jurídicos adversos.

Al igual que en el caso de la creación de perfiles, la ley chilena no contiene figuras creadas específicamente para abordar la problemática de la toma automatizada de decisiones. La única mención relevante al tratamiento automatizado de datos se encuentra en el Artículo 2º letra o) de la Ley N.º 19.628, que al definir tratamiento de datos personales aclara que este puede ser o no ser de carácter automatizado.

El proyecto de ley en discusión, por su parte, por medio de las indicaciones introducidas por el Ejecutivo, establece el derecho a oponerse a valoraciones personales automatizadas, estableciendo en su artículo 8 bis que "[e]l titular de datos tiene derecho a oponerse a que el responsable adopte decisiones que le conciernan, basadas únicamente en el hecho de realizarse a través de un tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles", con algunas excepciones.

Esta redacción también se encuentra fuertemente inspirada en el GDPR, el cual en su artículo 22 establece que "[t]odo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Por último, a pesar de encontrarse en la sección de considerandos, la sección 71 de este apartado establece que el titular tiene derecho a "a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión".

La redacción del artículo es prácticamente idéntica. Una diferencia significativa es que el GDPR permite impugnar la decisión, mientras que la norma propuesta en el proyecto chileno solo permite solicitar la revisión de la decisión. Por otra parte, el articulado del proyecto chileno no exige como requisito del derecho a oposición que la decisión automatizada produzca efectos jurídicos al titular o lo afecte significativamente.

Al menos dos de las empresas estudiadas realiza toma de decisiones automatizadas con base en los datos que recolecta de sus usuarios. Facebook utiliza la información recolectada del comportamiento del usuario y lo utiliza para entregarle un servicio personalizado. De esta forma, se toman decisiones respecto de qué tipo de contenido priorizar o mostrarle en su timeline. Del mismo modo, esa información también se utiliza para que los anunciantes puedan mostrarle publicidad dirigida. En ambos casos se toman decisiones que pueden resultar arbitrarias o discriminatorias. Por ejemplo, Facebook fue multado en Estados Unidos porque sus anunciantes utilizaron el perfilamiento de usuarios para hacer publicidad específica con base en criterios discriminatorios, tales como raza, edad, nacionalidad y discapacidad (NFHA s.d.).

Del mismo modo, la toma de decisiones automatizadas para la contratación laboral implica el riesgo de replicar ciertos sesgos de selección, con base en criterios como el género, como ha sucedido en experiencia comparada[25].

En el grupo focal se dio una interesante discusión sobre el tema, en la cual los participantes pusieron énfasis en la falta de transparencia en la forma en que se toman estas decisiones. Un académico señaló que:

> Hoy muchos organismos públicos están usando algoritmos, pero no hay forma para los usuarios de saber qué tipo de decisiones, bajo qué condiciones y bajo qué parámetros se están tomando esas decisiones. Por ejemplo, si un banco me niega un préstamo y no me dan ninguna explicación. Es muy distinto cuando son herramientas para tomar decisiones que cuando toman decisiones directamente.

Del mismo modo, un miembro de la sociedad civil añadió que: "El problema es que el algoritmo se protege por propiedad intelectual, y eso agrega una capa de opacidad a los esfuerzos de fiscalización".

---

25 Ver, por ejemplo, Dastin, (2018).

4.2. Lo que está inadecuadamente regulado

4.2.1. Excepciones al principio del consentimiento

Con la finalidad de proteger a los individuos y asegurar que estos mantengan el control de sus datos personales, la legislación establece que —por regla general— terceros distintos al titular no podrán tratar sus datos personales, a menos que el titular consienta con dicho tratamiento. Para que este consentimiento resulte válido, de acuerdo con el Artículo 4º de la Ley N.º 19.628, el titular debe ser informado sobre el propósito del procesamiento de sus datos y su eventual publicación y la autorización debe realizarse de forma expresa y por escrito. Del mismo modo, el titular siempre podrá revocar su consentimiento, aunque sin efecto retroactivo.

Una de las principales debilidades de la Ley N.º 19.628 es que contempla una serie de excepciones al requisito de consentimiento por parte del titular, las cuales, por su carácter excesivamente amplio, horadan gravemente su capacidad de protección. Jijena (2010) ha llegado al punto de aseverar que estas disposiciones generan el efecto de que la desprotección se transforme en la regla general y la protección en la excepción.

La excepción más problemática es la contenida en el inciso quinto del mismo Artículo 4º, el cual señala que:

> [n]o requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Esta excepción no solo implica que los datos obtenidos de fuentes accesibles al público podrán ser tratados sin el consentimiento del titular, sino que el responsable de base de datos no estará obligado a respetar la finalidad para la cual esa información fue recolectada, ni estará obligado a guardar reserva respecto de ella, y que se limita gravemente el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (Alvarado 2014).

La jurisprudencia ha hecho una interpretación excesivamente amplia de esta excepción, estableciendo que cualquier información que se encuentre disponible en internet o a la que se pueda tener acceso mediante un pago constituye una fuente accesible al público. Así, en la Sentencia Rol N.º 5.243 del año 2015, la Corte Suprema de Chile confirmó que la existencia del sitio 24x7datos, en donde era posible averiguar el nombre de una persona ingresando su número de rol único nacional (número de identidad), o averiguar este número a partir del nombre, no era ilegal, por encontrarse esta información en una fuente accesible al público.

Otra excepción puede encontrarse en el inciso sexto del mismo artículo, que establece que:

> [t]ampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

Por último, el Artículo 20 establece que: "[e]l tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular". Sin embargo, no existe un nivel adecuado de precisión respecto de si dichas competencias deben estar expresamente establecidas con respecto al tratamiento de datos o si se trata de una habilitación genérica y relativamente amplia. Lo anterior ha dado pie a que los organismos públicos interpreten que siempre están habilitados para tratar datos personales, incluso sensibles, en la medida que dicho tratamiento verse sobre alguna materia relacionada con sus competencias.

El proyecto de ley no parece subsanar estas deficiencias. El proyecto no aprovechó la oportunidad para limitar aquellas fuentes que se consideran accesibles al público a una lista cerrada de casos. En vez de ello, al igual que la ley actual, el proyecto opta por una definición amplia de esta categoría, entendida como "todas aquellas bases de datos o conjuntos de datos personales, públicos o privados, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, siempre que no existan restricciones o impedimentos legales para su acceso o utilización". No obstante, el articulado propuesto exige que la consulta deba realizarse de forma lícita, y el Artículo 13, letra a, establece que para poder hacer

un uso legítimo de esta excepción es necesario que el "tratamiento esté relacionado con los fines para los cuales fueron entregados o recogidos".

Respecto del tratamiento por parte de organismos públicos también se identifica una leve mejora. El Artículo 20 del proyecto en discusión establece que "[e]s lícito el tratamiento de los datos personales que efectúan los órganos públicos cuando se realiza para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias". La mención al cumplimiento de funciones legales, dentro del ámbito de sus competencias, entrega elementos interpretativos para argumentar que dicha habilitación debe encontrarse entre las atribuciones que la ley expresamente confiere al organismo público en cuestión y que esta habilitación no puede ser inferida indirectamente a través de competencias genéricas de la administración pública.

Por último, dentro de las excepciones más relevantes contenidas en el proyecto de ley se encuentra el hecho de que este incorpora una excepción no contenida en la Ley N.º 19.628. El Artículo 13, letra e, de la propuesta, establece que no se requerirá del consentimiento del titular "[c]uando el tratamiento sea necesario para la satisfacción de intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular".

Si bien el GDPR también considera la excepción del interés legítimo, el considerando (47) establece una serie de elementos que permiten interpretar de forma más precisa y otorgar más certeza jurídica al precepto. De esta forma, se establece que:

> [e]l interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. [...] En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin [...].

Del mismo modo, el Artículo 6 del GDPR no contiene una excepción amplia al principio del consentimiento por el hecho de que la información

haya sido obtenida en una fuente accesible al público. Respecto al tratamiento por parte de organismos públicos, el Artículo 6 establece un criterio más restrictivo, exigiendo que el tratamiento sea necesario para el ejercicio de poderes públicos conferidos al responsable del tratamiento.

El reglamento europeo contiene excepciones mucho más acotadas al principio de licitud, otorgando un estándar de protección mayor a la legislación vigente en Chile, pero también superior al propuesto por el proyecto de ley de datos personales.

La necesidad de contar con el consentimiento del titular y sus excepciones también suscitó una importante discusión en el grupo focal. Así, un abogado especializado en la materia señaló que "la fuerza del consentimiento está bajando, el consentimiento por escrito está un poco anacrónico. La ley se centra mucho el consentimiento y pierden fuerza otros habilitantes de licitud". Del mismo modo, un representante de la sociedad civil añadió que "lo que pasa es que se carga la responsabilidad sobre el titular y eso le resulta perjudicial".

4.3. Ámbito territorial de aplicación de la normativa

En Chile, la regla general es la aplicación del principio de territorialidad de la ley. Las excepciones a este principio están establecidas en el Artículo 6º del Código Orgánico de Tribunales e incluyen la persecución de delitos tales como la piratería, aquellos cometidos por un agente diplomático en ejercicio de sus funciones, aquellos que atenten contra la soberanía o contra la seguridad exterior del Estado, entre otros. En esta lista no se hace mención de ninguna disposición relativa a la protección de datos personales. Lo mismo ocurre respecto de la regulación de situaciones jurídicas de carácter civil, contenidas en el Código Civil.

Del mismo modo, la Ley N.º 19.628 no se pronuncia sobre la posibilidad de realizar una aplicación de sus disposiciones de carácter extraterritorial. Por lo mismo, es necesario entender que las disposiciones de la Ley N.º 19.628 solo se pueden hacer efectivas respecto del tratamiento de datos personales que tenga lugar al interior del territorio de la República y que las sentencias relativas a la materia solo podrán hacerse efectivas respecto de responsables de bases de datos que tengan domicilio constituido en Chile.

Si bien el proyecto de ley original no contenía ninguna disposición relativa a la aplicación extraterritorial, durante la tramitación legislativa

se incluyó un inciso final al Artículo 14, que regula los deberes de los responsables de bases de datos. De esta forma, se estableció que:

> "[a]demás de las obligaciones señaladas en el inciso anterior, el responsable de datos que no tenga domicilio en Chile y que realice tratamiento de datos de personas que residan en el territorio nacional, deberá señalar y mantener actualizado y operativo, un correo electrónico u otro medio de contacto idóneo para recibir comunicaciones de los titulares de datos y de la Agencia de Protección de Datos Personales".

Es discutible que esta obligación permita extender la aplicación de las decisiones de una futura autoridad pública de control de datos personales, o de los tribunales chilenos, más allá de las fronteras nacionales. No obstante, constituye un primer paso para al menos evitar que las EMNBD que operen en Chile se puedan desligar completamente de su vínculo con la legislación nacional.

Un panorama distinto presenta el GDPR, que en su Artículo 3 establece que "[e]l presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no". De esta forma, se aplican las disposiciones del GDPR al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. La Unión Europea sí se ha propuesto explícitamente la aplicación extraterritorial de su legislación de protección de datos personales. De esta forma, su capacidad de hacer efectiva su normativa y hacer rendir cuentas a las EMNBD se encuentra en una situación mejorada respecto de la legislación chilena.

Es posible que Europa pueda hacer efectiva su legislación más allá de sus fronteras debido al tamaño y peso de su mercado, que le permite tener un real poder de negociación con GAFAM. Es por ello que, desde su entrada en vigencia, el GDPR ha tenido un efecto expansivo, teniendo en consideración que muchas empresas del ecosistema digital han decidido transformar el cumplimiento de sus disposiciones en su estándar

global, independiente de la jurisdicción a la que pertenezcan cada uno de sus usuarios.

Este análisis es particularmente relevante en el caso de Facebook, que es la única de las cuatro empresas estudiadas que no cuenta con domicilio legal en Chile. De esta forma, incluso de aprobarse el proyecto de ley de datos personales, seguirá existiendo un importante desafío respecto a la aplicación de las normas chilenas de protección de datos personales realizado por Facebook, ya que este tratamiento estaría sujeto a la jurisdicción de otros países.

En el grupo focal, un representante de la industria señaló que:

> Es un tema súper complicado y es transversal a todas las áreas del derecho. Si el infractor no tiene activos en el país, vas a tener que hacerlo afuera, eso no lo vas a cambiar incluso teniendo un representante en Chile de Facebook para poder notificarlo. Una cosa es notificar y la otra es tener activos que embargar.

Del mismo modo, un académico participante de la discusión acotó que este no es un problema exclusivo de la protección de datos personales, sino que también atingente a otras áreas del derecho, así, explicó: "No estamos teniendo esta discusión en derecho al consumidor y otros. Quizá debería solucionarse a nivel general de derecho internacional privado".

5. Evaluación de las capacidades de las Autoridades de Protección de Datos

El hecho de que Chile carezca de una autoridad administrativa de control en materia de protección de datos personales implica que aquellos individuos que vean vulnerados sus derechos deben recurrir a los tribunales ordinarios de justicia. Esta vía procesal implica una barrera de entrada excesivamente alta para la mayoría de los individuos, ya sea por los costos económicos del litigio, el requisito de contar con patrocinio de un abogado, o la duración que un litigio de estas características suele tener. Todos estos factores han repercutido en que la Ley N.º 19.628 haya sido objeto de un número reducido de casos llevados ante tribunales, lo que ha generado una carencia de jurisprudencia relevante en la materia. Del mismo modo, los titulares se han visto privados de un mecanismo accesible, expedito y eficiente para hacer efectivos los derechos que la Ley N.°19.628 les garantiza.

Otro aspecto que ha desincentivado la aplicación de la Ley N.º 19.628 es el bajo monto de las multas que esta prevé. Para lograr que un responsable de bases de datos sea sancionado por la infracción de alguna de las disposiciones de la ley de datos personales, es necesario que el titular interponga una acción judicial conocida como *habeas data*, la cual procede en aquellos casos en que el responsable del banco de datos no se pronuncie sobre una solicitud de información, modificación, cancelación o bloqueo en un plazo de dos días hábiles o cuando esta sea denegada.

Este procedimiento es breve y sumario. De acogerse la reclamación, la sentencia podrá aplicar una multa de una a diez unidades tributarias mensuales (686 dólares aproximadamente), o de diez a cincuenta unidades tributarias mensuales (entre 686 y 10 299 dólares) si los datos eran relativos a obligaciones de carácter económico, financiero, bancario o comercial. Como se aprecia, el monto de las multas no resulta lo suficientemente significativo para tener un carácter disuasivo y una EMNBD del nivel de las GAFAM o de una empresa consolidada que fácilmente pueda incorporar dichas multas como un costo de operación.

El Comité de Evaluación de la Ley publicó un informe en el año 2016, relativo a las deficiencias de la regulación chilena de protección de datos personales. El informe incluyó en su metodología la realización de una serie de entrevistas a expertos en la materia. Uno de ellos, al ser consultado sobre la idoneidad del mecanismo de control judicial contenido en la legislación vigente, expresó que "[l]a ley vigente, es obvio que tiene problemas del punto vista que no tiene mecanismos para hacer efectivos los cumplimientos. Hoy día el costo transaccional de reclamar la infracción del derecho es tan alto que la gente no reclama" (2016, 53).

Por último, cabe mencionar que la Ley N.º 20.285 otorgó al Consejo para la Transparencia la competencia de velar por el adecuado cumplimiento de la Ley N.º 19.628, por parte de los órganos de la Administración del Estado. Sin embargo, no existe certeza del alcance del verbo rector 'velar' y la entrega de esta facultad no estuvo acompañada de ninguna capacidad de sanción ante el incumplimiento de las decisiones del Consejo. Por lo mismo, hasta el momento, este organismo se ha limitado a oficiar, solicitar información y emitir recomendaciones a otros organismos públicos en materia de procesamiento de datos personales. Sin embargo, no es posible aseverar que constituya una verdadera instancia de control para los organismos públicos.

Esta deficiencia crucial de la ley chilena dificulta gravemente la aplicación de la legislación y su capacidad para hacer rendir cuenta a las cuatro categorías de EMNBD en estudio.

Corregir esta falencia es uno de los principales objetivos del proyecto hoy en discusión en el Senado chileno. El proyecto original consideraba la creación de una Agencia de Protección de Datos Personales con un nivel de autonomía funcional, pero dependiente del Ministerio de Hacienda. Luego, por medio de una indicación sustitutiva en julio de 2018 el gobierno de Sebastián Piñera optó por asignar al Consejo para la Transparencia la tarea de transformarse en la nueva Agencia de Protección de Datos, pasando a llamarse Consejo para la Transparencia y la Protección de Datos Personales. Aunque parecía ideal que la nueva institucionalidad siguiera un modelo similar a la Agencia Española de Protección de Datos, es decir, un organismo autónomo, de carácter técnico, con patrimonio propio y con independencia de otros poderes políticos, gobiernos sucesivos argumentaron que esa opción estaba descartada por razones presupuestarias.

Así, correspondió al Senado decidir si inclinarse por el Consejo para la Transparencia o por una nueva autoridad dependiente del Ministerio de Hacienda. Ambos modelos contaban con ventajas y desventajas. La agencia dependiente de Hacienda contaba con mayor nivel de especialidad técnica, siendo un organismo dedicado de forma exclusiva a la protección de datos personales, pero con un nivel de independencia reducido, al depender jerárquicamente de un ministerio. Por otro lado, el Consejo para la Transparencia cuenta con un importante nivel de autonomía, pero no sería un organismo especializado. Si bien es cierto que la protección de datos personales y el acceso a la información pública no son materias necesariamente excluyentes, sí es cierto que responden a énfasis en bienes jurídicos particulares, sujeto a los sesgos y prioridades de formación de los profesionales que se dedican a cada área. El día 5 de agosto de 2019, la Comisión de Constitución del Senado —en voto dividido— decidió que el Consejo para la Transparencia se transformará en la nueva Agencia de Protección de Datos Personales (Biobío 2019).

El Artículo 31 del proyecto establece las competencias que le serán entregadas a la Agencia de Protección de Datos Personales. Entre las más relevantes se encuentran:

> a) Aplicar e interpretar administrativamente las disposiciones legales y reglamentarias cuyo cumplimiento le corresponde

> vigilar, e impartir instrucciones de carácter general a las personas naturales o jurídicas que realicen tratamiento de datos personales. Las instrucciones generales que dicte deberán ser emitidas previa consulta pública efectuada mediante su página web institucional.
>
> b) Fiscalizar y velar por el cumplimiento de los principios, derechos y obligaciones establecidos en esta ley. Para efectos de fiscalización se podrá solicitar la entrega de cualquier documento, libro o antecedente que sea necesario.
>
> c) Resolver las solicitudes y reclamaciones que formulen los titulares en contra de los responsables de datos.
>
> d) Investigar y determinar las infracciones en que incurran los responsables de datos y ejercer, en conformidad a la ley, la potestad sancionatoria [...]
>
> h) Desarrollar programas, proyectos y acciones de difusión, educación, promoción e información dirigidos a la ciudadanía y a los responsables de datos, en relación al respeto y protección del derecho a la vida privada y a la protección de los datos personales.
>
> [...]
>
> ñ) Resolver las solicitudes o consultas relativas a si una determinada base de datos o conjunto de datos es considerada fuente de acceso público e identificar categorías genéricas que posean esta condición.

Esta facultad sancionatoria está acompañada con un aumento de las multas y otras sanciones, con el objetivo de dotar a la legislación de herramientas que efectivamente resulten disuasivas a la hora de hacer efectivas las disposiciones de la legislación.

De esta forma, el Artículo 39 establece que:

> a) Las infracciones leves serán sancionadas con amonestación escrita o multa de 1 a 50 unidades tributarias mensuales.
>
> b) Las infracciones graves serán sancionadas con multa de 51 a 500 unidades tributarias mensuales.
>
> c) Las infracciones gravísimas serán sancionadas con multa de 501 a 5000 unidades tributarias mensuales.

Del mismo modo, se establece la creación de multas accesorias en caso de infracciones gravísimas reiteradas, consistente en la suspensión de las operaciones y actividades de tratamiento de datos que realiza el responsable de datos, hasta por un término de 30 días y la creación de un Registro Nacional de Cumplimiento y Sanciones.

Conclusiones y Recomendaciones

Luego de la descripción y análisis de las políticas de privacidad y condiciones de uso de Facebook, Falabella, PedidosYa y AIRA, y considerando el panorama normativo y legislativo nacional, se puede concluir que, haciendo eco de la tendencia global, en Chile las EMNBD, sin importar el grado de consolidación que tengan en el mercado, consideran el dato como un activo estratégico y, como tal, la principal finalidad que estas tienen para su tratamiento es atraer nuevos usuarios y generar nuevos productos al mínimo costo.

Como se pudo observar, el éxito de una EMNBD está proporcionalmente relacionado con la capacidad que esta tiene para recopilar datos y por, sobre todo, interpretar la información derivada o inferida de estos. Como consecuencia de lo anterior, la estrecha relación existente entre el Big Data y la IA seguirá en aumento y en evolución, ya que con los macrodatos se pueden capacitar sistemas de inteligencia artificial como redes neuronales y modelos estadísticos, con el fin de predecir algunos acontecimientos y comportamientos, lo cual es información considerada de alto valor para este tipo de empresas, ya que les permite entender y predecir el flujo del mercado actual.

La principal fuente de datos de las EMNBD, de acuerdo con lo indicado en sus respectivas políticas, es por medio de la información recolectada directamente de sus usuarios, de terceros (desarrolladores de aplicaciones para teléfonos móviles, socios estratégicos, etcétera) y mediante el monitoreo de usuarios mediante *cookies*. Respecto a los datos recolectados directamente de sus usuarios, aún existen empresas que solicitan información sobre el género de la persona de forma obligatoria para condicionar el uso de los servicios al otorgamiento de esta información (Facebook). Mientras que, en el caso de la información obtenida por medio de terceros, las empresas no otorgan información sobre cómo fiscalizan y llegan a la convicción de que los datos fueron obtenidos de forma legítima.

El *webtracking* a través de *cookies* ha generado nuevas fuentes de recolección de datos y, en consecuencia, nuevas finalidades para su tratamiento, las cuales van más allá de solo otorgar al usuario acceso al servicio. Es más, en la actualidad el tratamiento de datos más apetecido y valioso para las EMNBD es el que se efectúa con la finalidad principal de elaborar perfiles de usuarios y estudios sobre su comportamiento de navegación. Sobre esto último, lamentablemente las empresas no transparentan la operación de sus algoritmos, ni las herramientas analíticas para la recolección y tratamiento de datos.

En virtud de estas consideraciones, se plantean múltiples preocupaciones a nivel nacional sobre la escasa regulación y fiscalización a las EMNBD. Esto obedece, por una parte, a una legislación obsoleta en materia de protección de datos vigente desde el año 1999, y por otra, a la inexistencia de una autoridad de control, independiente y especializada, encargada de aplicar la normativa vigente.

En este escenario, se presentan las siguientes recomendaciones:

1. Las EMNBD deben transparentar la relación existente entre ellas con las GAFAM. En aquellos casos donde la empresa otorga la posibilidad de registro mediante la interconexión con la cuenta de Facebook (PedidosYa) o Google (AIRA), se deben hacer explícitas las consecuencias que conlleva esta acción para el tratamiento de datos personales. En este contexto, tanto el estado como la sociedad civil deben promover campañas comunicacionales tendientes a educar a la ciudadanía respecto a los alcances y principales efectos de la aceptación de políticas y condiciones de uso.
2. Sobre las finalidades en el tratamiento de datos, las EMNBD deben describir de forma clara y explícita las finalidades para cada tipo de tratamiento de datos. Asimismo, tampoco deben limitarse a efectuar una referencia general sobre la presencia de *cookies* en el portal, sino que además se sugiere que informen sobre el tipo de *cookies* que utilizan (persistente, analítica, de personalización, etcétera), así como también la individualización de las herramientas de recolección y análisis de datos de las que se valen (práctica adoptada por PedidosYa), y entregar herramientas para la oposición a ese tratamiento, sin perder acceso al servicio.

3. Se debe promover el desarrollo jurisprudencial de los conceptos de 'vida privada', 'dato personal', 'dato sensible', 'responsable del tratamiento de datos', 'fuente de acceso público', entre otros. Lo anterior se estima necesario, debido a que la judicatura en escasas ocasiones ha podido razonar y construir un criterio acorde a los tiempos actuales. Esto se debe, por una parte, a la dificultad y falta de pericia para la determinación del bien jurídico protegido en los ambientes tecnológicos y, por otra parte, debido a la ineficacia del *habeas data* de la Ley N.º 19.628, de 1999, por ser un procedimiento únicamente judicializado y de extensa duración y costos.
4. Establecer un marco jurídico e institucional con las capacidades y facultades suficientes para fiscalizar las actividades de las empresas GAFAM y establecer multas verdaderamente disuasivas que no terminen por ser incorporadas al costo de operación de las empresas.

Referencias

Accenture Technology Vision. *The Post-Digital era is upon us: Are you ready for what's next?* 2019. Consultado marzo 25, 2019. https://www.accenture.com/_acnmedia/pdf-97/accenture-technology-vision-2019-executive-final-brochure.pdf

AIRA. Condiciones de uso para postulantes. AIRA, 2019. Consultado marzo 25, 2019. https://shared-files.airavirtual.com/terminos-postulantes

Alvarado, F. Las fuentes de acceso público a datos personales. *Revista Chilena de Derecho y Tecnología*, 3(2), 2014: 205-226. doi: 10.5354/0719-2584.2014.33276

APEC. *Privacy Framework, APEC Secretariat*. 2005. Consultado marzo 25, 2019. http://www.apec.org/Groups/Committeeon-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

App Annie. Top App Matrix. 2019. Consultado marzo 25, 2019. https://www.appannie.com/dashboard/home/

APEC. *Cooperation arrangement for cross-border privacy enforcement*. 2009. Consultado marzo 25, 2019. http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf

Becker Castellaro, Sebastián y Romina Garrido. La biometría en Chile y sus riesgos. *Revista Chilena de Derecho y Tecnología*, 6(1), 2017. Doi: 10.5354/0719-2584.2017.45825

Biobío (2019). *Comisi*ón de Constitución del Senado aprueba que CPLT *proteja los datos personales*. Consultado marzo 25, 2019. https://www.biobiochile.cl/noticias/nacional/chile/2019/08/05/comision-de-constitucion-del-senado-aprueba-que-cplt-proteja-los-datos-personales.shtml

Boyd, Danah y Kate Crawford. Six Provocations for Big Data. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. *SSRN Electronic Journal*, *123*(1), 2011. Doi: 10.2139/ssrn.1926431

Büchi, Moritz, Eduard Fosch, Christoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi, Salome Viljoen. *Chilling Effects of Profiling Activities: Mapping the Issues*. 2019. Doi: http://dx.doi.org/10.2139/ssrn.3379275

Cámara Nacional de Comercio, Servicios y Turismo (CNC) (2019). *Ventas de comida rápida crecieron un 5.4% durante el primer trimestre 2019*. Consultado julio 25, 2019. https://www.cnc.cl/ventas-de-comida-rapida-crecieron-un-54-durante-el-primer-trimestre-2019/

Canales, María Paz y Pablo Viollier. La compatibilidad de la retención general de metadatos y el respeto a los derechos fundamentales: el caso del decreto espía. En Figueroa, R. (Ed.). *Anuario de Derecho Público de la Universidad Diego Portales* (pp. 155-171). Santiago: Uuniversidad Diego Portales, 2018. Consultado julio 25, 2019. http://derecho.udp.cl/wp-content/uploads/2019/01/AnuarioDerPub_2018_INTERIOR_ok.pdf

Canales, María Paz.¿Quién defiende tus datos? La problemática acción de Subtel. *Derechos Digitales*. 2019. Consultado julio 25, 2019. https://www.derechosdigitales.org/13302/la-problematica-accion-de-subtel/

Cerda, Alberto. *Legislación sobre protección de las personas frente al tratamiento de datos personales. Material de estudio del Centro de Estudios en Derecho Informático*. Santiago: Universidad de Chile, 2012.

Chile, Cámara de Diputados. Proyecto de Ley que Moderniza la legislación tributaria (23 agosto 2018). Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12561&prmBOLETIN=12043-05

CIPER. El empleado de Enrique Correa que opera como asesor de los senadores. *CIPER*. 2019. Consultado julio 25, 2019. https://ciperchile.cl/2019/05/06/el-empleado-de-enrique-correa-que-opera-como-asesor-de-los-senadores/

CNN Chile. *Director regional de Facebook y primer Innovation Lab en Chile: En muchos atributos son muy parecidos al primer mundo*. 2019. Consultado julio 25, 2019. https://www.cnnchile.com/lodijeronencnn/facebook-innovation-lab-chile-director-regional_20190228/

Comité Evaluación de la Ley. Evaluación de la ley 19.628 Protección de la Vida Privada. http://www.evaluaciondelaley.cl/foro_ciudadano/site/artic/20151228/asocfile/20151228124429/informe_final_ley_19628_con_portada.pdf

Contreras, Pablo. Propiedad de datos personales. *Apuntes de derechos*. 2019. Consultado julio 25, 2019. https://www.pcontreras.net/blog/propiedad-de-datos-personales

Dastin, Jeffrey. *Amazon scraps secret AI recruiting tool that showed bias against women. Reuters*. 2018. Recuperado de https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

Decreto 100, Fija el texto refundido, coordinado y sistematizado de la Constitución política de la República de Chile [Ministerio Secretaría General de la Presidencia] (17 septiembre 2005). https://www.leychile.cl/Navegar?idNorma=242302&r=1

Diaz, David y Mohamed Zaki. *Innovaci*ón en Modelos de Negocios Basados en Datos. Santiago, Chile, 2015.

DW. EE.UU. multa a Facebook con US$5.000 millones por violación de privacidad. *El Mostrador*. 2019. Consultado julio 25, 2019. https://www.elmostrador.cl/dia/2019/07/24/eeuu-multa-a-facebook-con-5-000-millones-por-violacion-de-privacidad/

Facebook. Política de datos s.d. Consultado julio 25, 2019. https://www.facebook.com/about/privacy/update

Facebook. ¿Cómo colabora Facebook con los proveedores de datos? s.d. a Consultado julio 25, 2019. https://www.facebook.com/help/494750870625830?ref=dp

Falabella. Tu cuenta s.d.a. Consultado julio 25, 2019. https://www.falabella.com/falabella-cl/page/comprar-terminos-condiciones?staticPageId=37900007&menu=comprar&srv=c5

Falabella. Quiénes somos s.d. b. Consultado julio 25, 2019. https://investors.falabella.com/Spanish/quienes-somos/default.aspx#section=about

Falabella. Canje de puntos. s.d. c Consultado julio 25, 2019. https://www.cmrfalabella.com/b2cfapr/CMRCORP/grafica/html/GRAFICACORP/PC/desc.html

Facebook. Tus preferencias de anuncios. s.d. d Consultado julio 25, 2019. https://www.facebook.com/ads/preferences

Facebook. ¿Cuáles son los productos de Facebook? s.d. e. Consultado julio 25, 2019. https://www.facebook.com/help/1561485474074139?ref=tos

Facebook. Por qué es mejor crear una página en Facebook. Facebook for Business. 2014. Consultado julio 25, 2019. https://www.facebook.com/business/news/LA-Por-que-es-mejor-crear-una-Pagina-en-Facebook-para-tu-negocio

Facebook. Removiendo el acceso a datos. *Facebook Newsroom*, 2019. Consultado julio 25, 2019. https://about.fb.com/ltam/news/2019/07/removiendo-el-acceso-a-datos/

Facebook. Ahora puedes ver y controlar los datos que las aplicaciones y sitios web comparten con Facebook. Facebook Newsroom. 2019a. . Consultado julio 25, 2019. https://about.fb.com/ltam/news/2019/08/ahora-puedes-ver-y-controlar-los-datos-que-las-aplicaciones-y-sitios-web-comparten-con-facebook/

Feldman, B. L., Adolphs, R. Marsella, S. Martinez, A., y Pollak, S. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest, 20*(1), 2019. Doi: https://doi.org/10.1177/1529100619832930

Gartner. (2012). *Big Data Analytics–Free Gartner Research*. 2012. Consultado julio 25, 2019. http://www.gartner.com/it-glossary/big-data/

Hartman, P. Zaki, M., Feldmann, N., y Neely, A. (2014). *Data for Big Business?* Cambridge Service Alliance Blog. Cambridge.

International Data Corporation. *Predicciones de la industria TI para el 2018 en Chile,* 2018. Consultado julio 25, 2019. https://innovacionchilena.cl/wp-content/uploads/2018/03/PPT-Predicciones-CL-2018.pptx-1.pdf

Jijena, Renato. (2001). Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628 de agosto de 1999. *Revista electrónica de derecho e informática*, (39), 2001. Consultado julio 25, 2019. https://libros-revistas-derecho.vlex.es/vid/intimidad-chile-analisis-19-628-1999-115523

Jijena, Renato. (2010). Actualidad de la protección de datos personales en América Latina. El caso de Chile. En Memoria del XIV Congreso Iberoamericano de Derecho e Informática, Monterrey, 2010. Consultado julio 25, 2019. http://biblio.juridicas.unam.mx/libros/6/2940/27.pdf

Ley N°19.628, Sobre protección de la vida privada [Ministerio Secretaría General de la Presidencia] (18 agosto 1999). https://www.leychile.cl/Navegar?idNorma=141599

Linio. *SACI Falabella informa adquisición del 100% de Linio y anuncia aumento de capital*. Linio, s.a. Consultado julio 25, 2019. https://www.linio.cl/sp/linio-grupo-falabella

López, Antonio. Web tracking e identificación de usuarios de Internet. *Incibe-Cert*, 2015. Consultado julio 25, 2019. https://www.incibe-cert.es/blog/web-tracking

Malik, Momim. Can algorithms themselves be biased? *Berkman Klein Center*. Consultado julio 25, 2019. https://medium.com/berkman-klein-center/can-algorithms-themselves-be-biased-cffecbf2302c

Montes, Carlos. Diez años de Facebook en Chile. *Diario La Tercera*, 2018. Consultado julio 25, 2019. https://www.latercera.com/tendencias/noticia/diez-anos-facebook-chile/106698/

National Fair Housing Alliance (s.d.). *Facebook Settlement* s.a. Consultado julio 25, 2019. https://nationalfairhousing.org/facebook-settlement/

Nava, Diana. Aira, la robot que te reclutará para tu nuevo trabajo. *El Financiero*, 2018. Consultado julio 25, 2019. https://www.elfinanciero.com.mx/tech/aira-la-robot-que-te-reclutara-para-tu-nuevo-trabajo

Newman Pont, Vivian y María Paula Ángel Arango. *Rendició*n de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital. Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2019. Consultado julio 25, 2019. https://www.dejusticia.org/publication/rendicion-de-cuentas-de-google-y-otros-negocios-en-colombia-la-proteccion-de-datos-digitales-en-la-era-digital/

OECD. *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*. OCDE, 2002. Consultado julio 25, 2019. http://www.oecd.org/sti/ieconomy/15590267.pdf

PedidosYa (s.d.). *Nosotros*. Consultado julio 25, 2019. https://www.pedidosya.cl/about/beneficios-restaurantes

PedidosYa (s.d.a.). Términos y condiciones. Consultado julio 25, 2019. https://www.pedidosya.cl/about/terminos-condiciones

Proyecto de Ley que Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales [Cámara de Diputados]. Marzo 15, 2017). https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07

Saldaña, María. El derecho a la privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego. *Revista Teoría* y realidad constitucional (28) 2001, 279-312.

Unión Europea. Parlamento Europeo y del Consejo. Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo. "Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ce (Reglamento general de protección de datos) 27 de abril de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Vega, Mayra y Deysy Ramírez. Startup en las redes sociales. *Revista Espacios*, 2018. Consultado julio 25, 2019. https://www.revistaespacios.com/a18v39n27/18392709.html

Velasco, Patricio y Pablo Viollier. *Información* financiera y discriminación laboral en Chile: un caso de estudio sobre B*ig Data*. Santiago: Derechos Digitales, 2016. Consultado julio 25, 2019. https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf

Viollier, Pablo. El estado de la protección de datos personales en Chile. Santiago: Derechos Digitales, 2017. Consultado julio 25, 2019. https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

We are Social y Hootsuite. Essential Insights into how people around the world use the internet, mobile, devices, social media, and e-commerce. *Global Digital Overview*, 2019. Consultado julio 25, 2019. https://www.slideshare.net/DataReportal/digital-2019-global-digital-overview-january-2019-v01

RENDICIÓN DE CUENTAS DE EMPRESAS CON MODELOS DE NEGOCIOS BASADOS EN DATOS EN COLOMBIA: LA PROTECCIÓN DE DATOS PERSONALES EN LA ERA DIGITAL

*María Paula Ángel Arango**
*Vivian Newman Pont***
*Daniel Ospina-Celis****

1. Introducción y selección de EMNBD

En un estudio previo titulado *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos en la era digital*, analizamos las políticas de privacidad de productos ofrecidos por treinta empresas con modelos de negocio basados en datos (EMNBD) que operan en Colombia. Para su análisis, clasificamos las distintas empresas en cuatro categorías: 1) grandes empresas de internet, 2) empresas intermedias, 3) *start-ups* y 4) empresas establecidas. En el primer grupo se encuentran Google, Amazon, Facebook, Apple y Microsoft (conocidas usualmente por el acrónimo GAFAM), todas ellas empresas que tienen gran capacidad de

* Abogada *Cum Laude* y politóloga de la Universidad de los Andes, Magíster en Derecho Administrativo de la Universidad del Rosario. Doctoranda en Derecho de la Universidad de Washington.

** Abogada de la Pontificia Universidad Javeriana, con posgrado en Derecho Administrativo (D.S.U.), Magíster en Derecho Público Interno (D.E.A.) de la Universidad de París II Panthéon-Assas y en Cooperación y Desarrollo de la Universidad de Barcelona. Actualmente se desempeña como directora de Dejusticia.

*** Abogado de la Universidad de los Andes e investigador de Dejusticia.

innovación y un amplio capital para invertir. Bajo la categoría de empresas intermedias se encuentran aquellas que, sin ser todavía grandes compañías de internet, no pueden considerarse *start-ups*. Algunas de ellas son Netflix, Deezer, Spotify, Waze o Uber. La tercera categoría, *start-ups,* corresponde a empresas que tienen una edad temprana, escalabilidad y un crecimiento exponencial (Entrepreneur 2018). Este tipo de empresas son, por lo general, de carácter nacional o regional como mucho. En el caso colombiano, empresas como Rappi, Cívico o Fluvip fueron consideradas como *start-ups* al momento de editar el estudio mencionado. Por último, en la categoría de empresas establecidas encontramos compañías como Almacenes Éxito, Unilever, Grupo Aval, Sura y Claro, empresas que, si bien existían antes de la era digital, se han adaptado a las nuevas tecnologías o han creado nuevos modelos de negocio basados en datos.

El criterio para escoger a las empresas intermedias fue su posición en el *ranking* creado por *App Annie*, el cual analiza las aplicaciones más descargadas en Colombia en AppStore y Google Play. Las aplicaciones que aparecieron en los top 10 de aplicaciones más descargadas en Colombia en los primeros 5 días de los meses de julio, agosto y septiembre, respectivamente, de 2018 son: Whatsapp, Tinder, Messenger, Facebook, Instagram, Facebook Lite, Netflix, Deezer, Google Drive, YouTube, Linkedin, Messenger Lite, AliExpress, Joom, 30 Days Fitness Challenge y 8fit Workouts and Meal Planner[1]. Si bien la mayoría de las *apps* antes mencionadas pertenecen a alguno de los GAFAM, las 7 aplicaciones restantes no son propiedad de estas empresas y, por lo tanto, su propietaria se consideró como una 'empresa intermedia'. En concreto, como empresa intermedia se estudió a: Match Group, LLC (Tinder); Netflix International B.V. (Netflix); Deezer S.A. (Deezer); Alibaba Group (AliExpress); SIA Joom Latvia (Joom); Bending Spoons S.p.A. (30 Days Fitness Challenge); y Urbanite Inc. (8fit Workouts and Meal Planner). Este grupo de empresas, debe decirse, se complementó con las siguientes cuatro empresas cuyas aplicaciones, si bien no se encuentran dentro del *ranking* de las más descargadas en Colombia durante los primeros 5 días de alguno de esos meses, sí eran muy populares en el país al momento de hacer el estudio: Easy Taxi Colombia S.A.S. (EasyTaxi); Spotify AB (Spotify); Uber B.V. (Uber) y Waze Mobile Limited (Waze).

1 Para una tabla en la que se organiza esta información, ver: Newman y Ángel (2019, 24).

En ese sentido, la categoría de empresas intermedias analizada estuvo compuesta por 11 empresas en total.

Por su parte, el criterio utilizado en el estudio para seleccionar la muestra de *start-ups* a analizar fue "su adscripción a Team Startup Colombia o al portafolio de startups dinámicas creado por INNpulsa Colombia" (Newman y Ángel, 2019, p. 25). Dada la gran cantidad de *start-ups* en el país, no se incluyeron la totalidad de iniciativas de ambos portafolios sino únicamente aquellas que todavía existen y de las cuales fue posible encontrar su política de privacidad. Adicionalmente a las seleccionadas de este modo, se incluyeron dos empresas que, aunque no se encuentran en los mencionados portafolios, ofrecen *apps* con modelos de tratamiento de datos interesantes para estudiar. Por último, la selección de las empresas establecidas se realizó a partir de las empresas más grandes en Colombia en los siguientes sectores: consumo masivo, *retail*, seguros, finanzas y telecomunicaciones. La muestra de EMNBD antes descrita no pretendió ser representativa, sino meramente ilustrativa del tipo de empresas que actualmente se encuentran recogiendo datos en Colombia. Los hallazgos aquí reportados corresponden al contenido que las Políticas de Privacidad revisadas tenían al momento de elaboración del documento *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos en la era digital*, y que corresponden a las fechas de "última actualización" reportadas en el Anexo 1 de dicho documento.

2. Forma de operar de las EMNBD que recolectan datos en Colombia

Al revisar las políticas de privacidad de los productos que ofrecen las 30 EMNBD estudiadas, se encontró que existen ciertos patrones en su forma de operar, los cuales fueron agrupados en las siguientes categorías: 1) fuente de datos, 2) tratamientos, 3) finalidades del tratamiento y 4) relación con las GAFAM.

2.1. Fuentes de datos

Con respecto a las fuentes de datos, se encontró que la mayoría de EMNBD que operan en Colombia tiene principalmente tres fuentes de datos. La primera se trata de los datos proporcionados por el usuario/cliente, los cuales usualmente se dan cuando este crea la cuenta o perfil, hace una compra o sube contenido a la plataforma o aplicación. En algunos

casos (Facebook y Tinder, por ejemplo), la información proporcionada puede constituir datos sensibles como ideología política, origen étnico, orientación sexual, creencias, intereses, etc. En otros casos, como el de Unilever, se reconoce que, si bien los servicios o productos solicitados pueden no implicar directamente la recopilación de categorías especiales de datos, estos sí podrían sugerir datos sensibles, como la religión o el estado de salud del titular de los datos.

La segunda fuente de información son los datos recolectados a través de *web tracking*. Estos incluyen datos sobre las aplicaciones, los dispositivos o el navegador utilizado por el usuario/cliente y sobre la actividad que ha realizado en la plataforma o aplicación. De la misma manera, incluyen datos sobre la ubicación del usuario, aun cuando no se utiliza la aplicación. Algunas empresas, como Duety, consideran que los datos recolectados por medio de *web tracking* no constituyen información personal, por no estar vinculados con el usuario sino con las direcciones de Protocolo de Internet (IP) y los identificadores similares del dispositivo utilizado. En forma similar, Apple señala que solo considerará las direcciones IP y los identificadores similares como información personal, si estos son así considerados en la respectiva legislación local.

Los datos proporcionados por socios estratégicos constituyen la tercera fuente de información más común. Este tipo de información no es recolectada por la plataforma o aplicación sino que proviene de un tercero, siendo algunos de ellos: 1) las compañías que prestan servicios a nombre de la empresa; 2) las empresas de publicidad que proporcionan servicios de *marketing* o investigación, 3) las plataformas de terceros en los que la empresa tiene una cuenta, 4) los terceros que procesan y analizan los datos personales en poder de las EMNBD, 5) las empresas a las que ellos les proporcionan servicios y 5) los burós de crédito que utilizan estas empresas en sus aplicaciones y plataformas.

Aunque menos utilizadas, las otras fuentes de datos identificadas fueron la adquisición de información de proveedores de datos externos, los datos de libre acceso en la web, el uso de sensores y dispositivos y el *crowdsourcing*.

2.2. Tratamientos

En cuanto a las formas de tratamiento de datos personales, se encontró que las EMNBD que operan en Colombia realizan principalmente dos actividades: 1) recolección y 2) análisis. La recolección se hace

usualmente por medio de distintas herramientas tecnológicas, las cuales tienen especificaciones técnicas que permiten de una u otra forma la recolección de datos. Las herramientas más comúnmente utilizadas son a) *cookies* de origen o de terceros: archivos que se envían al computador de un usuario cuando visita un sitio web, los cuales permiten que el sitio reconozca al ordenador cuando vuelve a visitarlo; b) identificadores de anuncios: cumplen una función muy similar a la de las *cookies* pero en un dispositivo móvil; c) etiquetas de pixel: permiten hacer seguimiento de una actividad (por ejemplo, cuando se visita un sitio o se lee un correo); d) kits de desarrollo de software (SDK por sus siglas en inglés): *cookies* o etiquetas de pixel en las apps; e) almacenamiento web del navegador: el sitio web almacena datos en el navegador de un dispositivo; f) cachés de datos de aplicación: información guardada en un dispositivo que permite que un sitio web funcione sin internet o que cargue más rápido; g) registros de servidor; h) direcciones URL de seguimiento: enlaces que permiten saber de dónde viene el tráfico en un sitio web. Es importante mencionar que existen distintas clases de *cookies*, los cuales recolectan información de diverso tipo. Una o varias clases de *cookies* son utilizadas por la EMNBD, dependiendo de los datos que desee recolectar.

Por otro lado, el análisis que se realiza sobre los datos es más uniforme. Principalmente, se realizan análisis de tipo descriptivo, encaminados a segmentar y clasificar a los usuarios de acuerdo con sus gustos, preferencias o intereses; o análisis de tipo prescriptivo, que buscan mejorar la experiencia del usuario en visitas futuras. En las políticas de privacidad de las aplicaciones, sin embargo, no se encuentra información técnica detallada que permita determinar las herramientas tecnológicas que cada producto utiliza para analizar los datos.

En contraste con la recolección y el análisis, es raro ver la venta o comercialización de datos como un tratamiento expresamente reconocido en las políticas de privacidad de las EMNBD que operan en Colombia. En particular, la única empresa que reconoce abiertamente esta clase de tratamiento es Cívico. En contraste, algunas de las empresas estudiadas (como Amazon, Facebook y Uber) indican expresamente que no participan en el negocio de la venta de la información de los clientes a terceros. Sin embargo, esto no es óbice para que las empresas señalen que en el caso de que la empresa sea adquirida por un tercero, los datos personales de los usuarios/clientes serán uno de los activos por transferir.

2.3. Finalidades

Del análisis de la política de privacidad de la muestra de 30 EMNBD, se encontró que son nueve las finalidades más comunes con las que se hace el tratamiento de datos personales. Estas son: 1) prestar un buen servicio, 2) comunicarse con el usuario, 3) desarrollar nuevos bienes o servicios, 4) administrar concursos, descuentos u otras ofertas, 5) adelantar investigaciones de mercado, 6) ofrecer contenido personalizado (como publicidad), 7) calcular el rendimiento de su contenido, 8) hacer estudios e investigaciones y 9) compartir información con terceros. Frente a esta última finalidad hay dos casos notables. El primero es el de 8fit Workouts and Meal Planner, cuya política de privacidad incluye una lista con los nombres de todas las aplicaciones que se conectan a ella, así como de todos los aliados con los que se comparte información. El segundo es Whatsapp, que a la hora de compartir datos con aplicaciones de terceros o con Facebook exige "respeto" por sus "instrucciones" y el cumplimiento de sus "condiciones en el momento de usar tu información en nuestro nombre".

Además de esas nueve finalidades más comunes, Cívico también incluye entre sus finalidades de tratamiento la configuración de una base de datos que pueda ser objeto de comercialización. En forma similar, Duety tiene entre sus finalidades la cesión de bases de datos. Por último, entre sus finalidades de tratamiento, Unilever incluye la de tomar decisiones automatizadas, entendidas como aquellas que se toman únicamente por medios automáticos, sin la intervención de seres humanos.

2.4. Relación con Google, Apple, Facebook, Amazon y Microsoft (GAFAM)

Por tratarse de las empresas de internet más grandes, la mayoría de aplicaciones tiene interacciones con alguno de los productos que ofrecen las GAFAM. En ese sentido, las EMNBD estudiadas se relacionan con las GAFAM, principalmente de cuatro formas: 1) la aplicación o página web permite el inicio de sesión por medio de algún tercero o red social (Facebook, Gmail, etc.), 2) la app o página web tiene botones sociales proporcionados por Facebook, Google+, Linkedin o Twitter, 3) la aplicación o plataforma web utiliza Google Analytics (servicio de análisis de datos de uso del sitio) o 4) dentro de sus socios publicitarios se encuentran compañías que hacen parte del grupo de Google. Estas relaciones le permiten, por

un lado, a la EMNBD hacer uso de datos personales proporcionados por los GAFAM y, por el otro, a los GAFAM acceder a la información en poder de las EMNBD.

3. Nivel de preparación del régimen actual de datos personales colombiano y de las autoridades competentes para enfrentar los retos que plantea la era digital

Teniendo en cuenta la forma en la que operan las EMNBD estudiadas, corresponde analizar ahora el nivel de preparación del régimen jurídico de protección de datos personales colombiano y de las autoridades competentes para proteger los datos personales frente a las fuentes, finalidades y formas de tratamiento propias de la era digital.

La protección de datos en Colombia se encuentra reconocida en el Artículo 15 de la Constitución Política y en dos leyes estatutarias que desarrollan el derecho fundamental al *habeas data*: la Ley Estatutaria 1266 de 2008, sobre el derecho a la protección de información financiera, crediticia, comercial, de servicios y proveniente de terceros países; y la Ley Estatutaria 1581 de 2012, sobre el tratamiento de datos personales en general. Estas leyes imponen principios básicos de tratamiento de datos como el principio de finalidad, de transparencia, de circulación restringida, de seguridad y de confidencialidad. En adición, crean categorías jurídicas especiales como los datos sensibles y los datos de niñas, niños y adolescentes.

Toda esta regulación, aunque novedosa en su momento, no tiene en cuenta temas propios de la era digital. Al realizar el estudio de las conductas desarrolladas por las EMNBD, mediante plataformas informáticas y la lectura detallada del contenido de la ley, se encuentra que la legislación actualmente aplicable en Colombia no cobija algunos fenómenos identificados al revisar la forma de operar de las EMNBD. Entre ellos, se pueden mencionar: 1) datos sensibles inferidos, 2) datos vinculados al IP, 3) uso de *cookies*, 4) web *crawling*, 5) comercialización de datos, 6) contenidos personalizados y 7) decisiones automatizadas. De igual forma, existen otras situaciones de uso de datos que, aunque están contempladas en la ley, su regulación no se encuentra acorde con las exigencias de la era digital (por ejemplo, lo relacionado con el consentimiento libre e informado).

3.1. Lo que no está regulado y debe regularse

Hay situaciones propias de la era digital que la regulación actual no tiene en cuenta y que implican desprotección de los titulares de datos personales.

Los datos sensibles inferidos y los datos de los que se infieren dichos datos sensibles presentan, a la luz del análisis de las prácticas de las EMNBD, un desafío para la legislación nacional. Según el Artículo 5 de la Ley 1581 de 2012, son datos sensibles "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación". Estos datos no necesariamente tienen que ser entregados por el titular, sino que su obtención puede darse por inferencia o por cruce de datos. En ese sentido, el tratamiento del dato sensible inferido, de igual manera que el del dato sensible, está prohibido en Colombia, salvo por las excepciones que contempla la misma ley (Artículo 6). Ahora bien, las prácticas de las EMNBD revelan que es posible utilizar datos no sensibles (por ejemplo, compras en Amazon.com) que, en conjunto con otros datos, permiten inferir datos personales sensibles (como la orientación sexual de una persona). La limitación de la legislación colombiana radica en que no tiene en cuenta que, por medio de ciertos datos personales, es posible obtener (inferir) nueva información de su titular. En este punto son urgentes desarrollos doctrinales y jurisprudenciales sobre el concepto de dato sensible establecido en el Artículo 5 de la Ley 1581 de 2012, para que quede claro que incluye, no solo los datos que pueden afectar la intimidad de una persona o generar su discriminación, sino aquellos que, si bien en principio no generan riesgo, al ser combinados con otros permiten inferir o derivar datos sensibles de su titular.

Otra de las cuestiones que no se encuentran reguladas por la legislación actual es la referente a los identificadores en línea, como las direcciones de protocolo de internet (IP), que permiten vincular a una persona por medio de la información de su dispositivo. La legislación colombiana no trae ninguna referencia directa al tema y no parece siquiera suponer que sea posible identificar a una persona determinada por medio de las direcciones IP y otros identificadores. Sin embargo, el literal c) del Artículo 3.º de la Ley 1581 de 2012, parece permitir que los identificadores en línea hagan parte del concepto de datos personales, en tanto define al dato personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas

o determinables". Teniendo en cuenta que el Reglamento General de Protección de Datos de la Unión Europea (GDPR, por sus sigla en inglés) (Artículo 4.º), la Ley de Privacidad del Consumidor de California (*California Consumer Privacy Act*, CCPA, por sus siglas en inglés) (sección 1798.140) y el Grupo de Trabajo del Artículo 29 ya reconocen las direcciones IP como datos personales, no parece inadecuado interpretar que la legislación colombiana engloba dentro de la categoría de dato personal a los identificadores web. En todo caso, lo cierto es que la ley nacional no trae una referencia directa a esta situación y, por tanto, deja abierta la puerta a que no se reconozca adecuadamente —como sucede en el caso de Apple, que no considere la dirección IP como dato personal—, si no lo hace así la legislación del país respectivo.

Por otro lado, de acuerdo con la caracterización que se hizo sobre la forma de operar de las EMNBD en Colombia, el uso de *cookies* es una de las prácticas más comunes en el mundo digital y por medio de las cuales se puede recolectar gran cantidad de información. En ese sentido, la legislación nacional debería estar diseñada para responder específicamente a las dinámicas y a los riesgos propios de esta herramienta tecnológica. Sin embargo, dado que la autoridad de protección de datos considera que una adecuada interpretación de la actual regulación de protección de datos es suficiente para proteger los derechos de los colombianos, esta ha conceptuado expresamente que "en Colombia no existe una regulación específica sobre el uso de *cookies*" (Concepto 14-218349-4-0, Superintendencia de Industria y Comercio -SIC- 2016). En esa medida, lo que se tiene actualmente es una ley que, al menos en su literalidad, trata la recolección de datos personales mediante *cookies* como cualquier otro tipo de tratamiento de datos personales. Por un lado, esto implica que no hay restricciones sobre las herramientas que se utilicen para dicha recolección, y mucho menos sobre el tipo de *cookies* que pueden ser implementadas. Por otro lado, esto quiere decir que a la recolección por medio de *cookies* le son aplicables las garantías, obligaciones y limitaciones legales del tratamiento de datos, entre ellas, por ejemplo, la obtención del consentimiento previo e informado del titular de los datos. Sin embargo, en este último punto es de notar el caso de la Unión Europea, en donde no solo existen limitaciones y excepciones al consentimiento del titular, específicamente en materia de *cookies*, sino que la regulación es incluso más estricta en lo que se refiere al consentimiento de las *cookies* para publicidad comportamental.

A la luz de este contraste, se considera indispensable que en Colombia se dé un mayor desarrollo doctrinal, jurisprudencial o legal sobre el uso de *cookies* para recolectar datos personales en línea, imponiéndose mayores limitaciones y exigencias de garantías para el otorgamiento del consentimiento, salvo que se trate de *cookies* que: 1) sean esenciales para el funcionamiento del servicio solicitado o 2) recolecten datos anonimizados o para uso agregado.

Otro de los fenómenos que parece no estar regulado es la comercialización de datos personales que, aunque en mucha menor medida, también se identificó en algunas de las políticas de privacidad de los productos de las EMNBD aquí estudiadas. Los datos tienen un valor económico y esto ha llevado a que en la era digital sea usual su compra y venta. Sin embargo, en Colombia la única referencia a la comercialización de datos personales se encuentra en el Artículo 269F del Código Penal y no en las leyes de protección de datos. Dicho estatuto establece lo siguiente:

> [...] el que, **sin estar facultado** para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, **venda**, intercambie, envíe, **compre**, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión [...] (énfasis propio).

A partir de dicho artículo se deduce que la comercialización de datos en archivos, ficheros o bases de datos está, en principio, permitida y que la prohibición de comercialización se da solo cuando no se está facultado para ello. Ahora bien, ¿cuándo se está facultado para ello? En virtud del principio de libertad, el consentimiento previo e informado podría facultar al responsable de la información para la comercialización de los datos personales.

Esta potestad de comercialización libre, sin embargo, puede suponer un riesgo de discriminación, vigilancia masiva y restricción de libertades civiles, especialmente a la luz de la práctica de los *data brokers*, que crean perfiles de los titulares de los datos. Evidentemente, esta situación contrasta con el CCPA de California, en el que se permite expresamente a los consumidores prohibir la venta de su información personal por parte de una empresa (referido en la ley como el derecho de *opt out*), y se le prohíbe a la compañía, salvo contadas excepciones, tomar represalias o discriminar a un consumidor en términos de precio

o calidad del bien o servicio ofrecido por ejercer este derecho. Además, dicha legislación prohíbe a las empresas vender la información personal de los consumidores menores de 16 años, salvo que el menor de edad (para los menores entre 13 y 16 años) o sus padres (para los menores entre 0 y 13 años) lo consientan afirmativamente (referido en la ley como el derecho de *opt in*). De igual forma, la falta de regulación de Colombia en la materia contrasta con en el caso de la Unión Europea, en donde, siendo conscientes del potencial que la venta de datos personales le da al perfilamiento, por medio del GDPR se ha intentado tanto promover la transparencia de la construcción de perfiles, como incentivar el carácter justo de los tratamientos de datos, incluido el *profiling*.

Teniendo en cuenta estos contrastes, es deseable que en Colombia se dé un mayor desarrollo doctrinal, jurisprudencial o legal sobre: 1) los tratamientos de datos que tengan como finalidad la comercialización de datos, para que estén sujetos a mayores garantías que las que ofrece el principio de finalidad, establecido en el literal b) del Artículo 4 de la Ley 1581 de 2014 y 2) el *profiling*, para que se asegure —al menos— la transparencia y el carácter justo del proceso de construcción de perfiles, que evite categorizaciones opacas basadas en datos errados o discriminatorios.

Adicionalmente, la legislación colombiana sobre protección de datos personales no contempla el derecho a la portabilidad de datos, como sí sucede en otros ordenamientos jurídicos. La portabilidad de datos implica que el titular de los datos pueda autónomamente 'trasladar' sus datos de un repositorio a otro. Lo anterior incluye dos cosas: que tenga acceso a una copia electrónica de todos los datos que haya proporcionado o que sean objeto de tratamiento —para transferirlos a otra empresa/responsable—, y que quien hace tratamiento de datos los transfiera directamente a otro, cuando medie instrucción del titular de los datos. A pesar de encontrarse reconocido en algunos instrumentos normativos como el GDPR (Artículo 20) y los Estándares iberoamericanos (Artículo 30), el derecho a la portabilidad de datos todavía suscita varias preguntas. Por ejemplo, ¿la portabilidad implica la transferencia de todos los datos o solo de aquellos proporcionados por el titular? ¿Puede un responsable conservar copias de la información sobre la que se han ejercido los derechos de portabilidad con fines de transferencia? Tanto expertos como la industria han dado respuestas disímiles a estas y a otras cuestiones. Por ejemplo, según los Estándares iberoamericanos, la portabilidad de datos no aplica a aquella información derivada u obtenida a partir de

análisis (Artículo 30.4). Por su parte, en septiembre de 2019, Facebook publicó un documento titulado *Portabilidad de datos y privacidad* en el que, más que sentar la posición de la compañía sobre el tema, formula preguntas difíciles sobre cinco aspectos relacionados con la portabilidad de datos (Egan 2019).

Otro tema sin regulación específica es el ofrecimiento de contenido personalizado (especialmente publicidad), que figuró como una de las finalidades con las que se realiza el tratamiento por parte de la mayoría de las EMNBD estudiadas. Si se revisa la Ley 1581 de 2012, resulta evidente que esta finalidad no tiene una regulación especial, más allá de las obligaciones generales propias de la finalidad para la que se puede realizar el tratamiento de datos personales. En ese orden de ideas, lo único que indica el régimen jurídico colombiano en este aspecto es que la finalidad debe ser legítima de acuerdo con la Constitución y ser informada al titular al momento de realizar la recolección de datos personales. Esta falta de regulación no tiene en cuenta que la personalización de contenidos se basa en el *profiling*, una práctica que, reiteramos, plantea riesgos para los derechos y libertades de cada persona. Además, desestima el hecho de que la publicidad personalizada no es siempre igual, sino que puede ser más o menos invasiva, según si se trata de publicidad contextual, segmentada o comportamental. Esta última es la que más afecta el derecho a la intimidad, en tanto se genera a partir del comportamiento de las personas en internet durante el tiempo.

En vista de estos riesgos, se considera indispensable que en Colombia se dé un mayor desarrollo doctrinal, jurisprudencial o legal sobre los tratamientos de datos que tengan como finalidad la provisión de contenidos personalizados (en particular cuando se trate de publicidad comportamental), para que, al igual que la comercialización de datos, estén sujetos a mayores garantías que las que ofrece el principio de finalidad.

Por último, la toma de decisiones automatizadas es otro de los fenómenos que, según la revisión de las políticas de privacidad aquí estudiadas, surge como resultado de la era digital y que no se encuentra regulada por la legislación de protección de datos colombiana. Frente a este caso, la regulación actual no atiende varios riesgos a la hora de recolectar datos con el fin de tomar decisiones automatizadas. Esta falta de regulación específica contrasta con lo señalado por los Principios Rectores sobre Empresas y Derechos Humanos y la Resolución de las Naciones Unidas sobre el Derecho a la Privacidad en la Era Digital

A/C.3/71/L.39. Y en especial, con lo previsto en el GDPR, el cual, le dio al titular de los datos la opción de oponerse al tratamiento automatizado si este produce efectos jurídicos sobre el titular de los datos o lo afecta significativamente de modo similar y, además, le exigió al responsable de los datos personales cumplir con ciertas obligaciones de participación del titular y de terceros humanos.

A la luz de estos desarrollos, se considera necesario que en Colombia se dé un mayor desarrollo doctrinal, jurisprudencial o legal sobre los tratamientos de datos que tengan como finalidad la toma de decisiones automatizadas, para que estén sujetos a mayores garantías que las que ofrece el principio de finalidad.

3.2. Lo que está inadecuadamente regulado

La era digital y el uso que realizan las EMNBD de las aplicaciones móviles y de las plataformas tecnológicas no han permitido únicamente fenómenos nuevos que requieren la creación de nuevo derecho, sino que también han modificado las condiciones en las que se deben aplicar las normas existentes. Este es el caso de la posibilidad de compartir datos personales para investigaciones académicas y del consentimiento previo, expreso e informado.

En primer lugar, el ordenamiento jurídico colombiano contempla la posibilidad de que el responsable del tratamiento de los datos los comparta con terceros para fines de investigación académica (específicamente fines históricos, estadísticos o científicos). En ese caso, en virtud del literal d) del Artículo 10 de la Ley 1581 de 2012, la autorización del titular no será necesaria y se podrá incluso realizar el tratamiento de datos personales sensibles siempre y cuando se adopten "las medidas conducentes a la supresión de identidad del Titular" (literal e), Artículo 6, Ley 1581 de 2012). Ahora bien, teniendo en cuenta el volumen de los datos sobre los cuales se realiza hoy en día el tratamiento, resulta insuficiente la exigencia de anonimizar los datos sensibles. Lo anterior porque, por más de que se tome esta precaución, si se cuenta con una cantidad considerable de datos personales, es posible reidentificar al titular. En contraste, en casos como el de la Unión Europea, el GDPR exige que la anonimización sea acompañada de la aplicación de un test de compatibilidad (*compatibility assesment*).

En segundo lugar, en Colombia el consentimiento se considera dado una vez se aceptan las políticas de privacidad de la plataforma

web o la aplicación. Estas políticas, aunque disponibles para todos los usuarios, resultan: 1) difíciles de leer debido a su extensión, 2) difíciles de entender debido a su complejidad y 3) difíciles de dimensionar en la práctica debido a su vaguedad. En adición, estas políticas no le permiten al titular superar los anteriores obstáculos, seleccionar los tratamientos y finalidades que desee autorizar y dejar por fuera aquellos con los que no esté de acuerdo. La información se presenta en bloque y debe ser aceptada o rechazada en su totalidad. Así las cosas, resulta dudosa la utilidad del consentimiento previo, expreso e informado, para proteger efectivamente los derechos de las personas y, en específico, el derecho a la protección de datos personales en un entorno de *big data*, en el que gran parte de las finalidades de tratamiento de los datos están aún por definirse. Esto contrasta con prácticas como las de la Unión Europea, que permiten, por ejemplo, "autorizar por separado las distintas operaciones de tratamiento de datos personales" (considerando 43, GDPR).

Por eso, es momento de que en Colombia se dé un mayor desarrollo doctrinal, jurisprudencial o legal sobre el consentimiento previo, expreso e informado del titular de los datos para que, al menos en los casos en los que el tratamiento de datos personales tenga como finalidad el *profiling*, la comercialización de datos, la provisión de publicidad comportamental o la toma de decisiones automatizadas, sea obligatorio solicitar el consentimiento de manera incondicionada y para cada finalidad específica, y sea obligatorio manifestarlo mediante una declaración o una clara acción afirmativa.

3.3. Ámbito de aplicación de la ley

Según el Artículo 2.° de la Ley 1581 de 2012, dicha normativa aplicará en dos escenarios: 1) "al tratamiento de datos personales efectuado en territorio colombiano" y 2) "cuando al responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales". La literalidad de este artículo parece indicar que la ley no es aplicable a empresas que no tengan su domicilio en Colombia (como todas las GAFAM y la mayoría de las empresas incluidas bajo la categoría "empresas intermedias"), pues el grueso de sus actividades de tratamiento de datos personales se realiza fuera de Colombia. De hecho, así lo interpretó inicialmente la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio. En 2014, al

analizar si la ley de protección de datos colombiana era aplicable a una empresa responsable de una red social, dicha Delegatura argumentó que la legislación colombiana sobre protección de datos no era aplicable pues "la recolección, el uso, el almacenamiento o supresión de los datos personales no se realiza dentro del territorio colombiano, puesto que las redes sociales no tienen domicilio en Colombia".

Sin embargo, en 2016 la SIC modificó su interpretación sobre el ámbito de aplicación de la Ley, y estableció que esta es aplicable a un sinnúmero de escenarios, entre los cuales se encuentra "el tratamiento de datos personales efectuado por proveedores de servicios de redes sociales establecidos fuera del país, a través de un 'medio' situado en territorio colombiano" (Superintendencia de Industria y Comercio, Concepto 14-218349-4-0 del 3 de marzo de 2016). En ese sentido, se ha entendido que por 'medio' la autoridad de protección de datos se refiere a las *cookies*, las cuales se almacenan en el computador del usuario al visitar un sitio web. El computador, y por lo tanto las *cookies,* se encuentran en territorio colombiano.

Ante este panorama, al momento de publicar *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos en la era digital* se expuso:

> consideramos que, si bien el segundo concepto de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio le dio un mayor alcance territorial a las obligaciones y garantías que contiene la Ley 1581 de 2012, todavía existe un amplio campo de mejora. Por ejemplo, sería interesante considerar el caso de la Unión Europea, en donde a partir del GDPR el ámbito de aplicación territorial de la regulación de protección de datos personales europea dejó de depender de la ubicación que tengan el responsable o encargado del tratamiento, sus establecimientos o los medios que utilice para tratar los datos. En contraste, pasó a depender de la ubicación de los titulares de los datos personales que son objeto de tratamiento (Newman y Ángel 2019).

En coincidencia con ese llamado, la Delegatura para la Protección de Datos de la Superintendencia de Industria y Comercio ha ampliado su interpretación sobre el ámbito de aplicación de la Ley. Así, en su Resolución 1321 de 2019, la Dirección de Investigaciones de la Delegatura para la Protección de Datos consideró que la Ley 1581 de 2012 es aplicable

a las empresas extranjeras que recolectan datos de nacionales colombianos en el territorio nacional. En dicha resolución, en la que se le dan órdenes concretas a Facebook para que cumpla la legislación nacional y garantice la seguridad de la información, la autoridad de protección de datos especifica que la normativa le es aplicable al "tratamiento de datos personales efectuado en territorio colombiano con independencia de si el Responsable o Encargado del Tratamiento se encuentra ubicado físicamente en el territorio de la República de Colombia". En adición, reconoce que, si bien buena parte del tratamiento de datos personales se hace mediante internet, "ello no significa que por ese fenómeno tecnológico desaparezca la obligación de cumplir las normas locales y de respetar los derechos humanos".

Siguiendo esta interpretación, la Delegatura para la Protección de Datos Personales expidió una segunda resolución en la que desarrolla de mejor manera el argumento sobre la aplicación de la ley a empresas no domiciliadas en Colombia. En la Resolución 21 478 de 2019, se le ordena a Uber garantizar la seguridad de los datos y el cumplimiento de la legislación nacional. Sobre la competencia indicó lo siguiente:

> [L]a Ley Estatutaria 1581 de 2012 se aplica a cualquier operación que se realice sobre piezas de información vinculadas o que puedan asociarse a personas naturales residentes o domiciliadas en la República de Colombia por parte, por ejemplo, de desarrolladores de aplicaciones móviles, aunque su sede principal no se encuentre en el territorio colombiano y aun cuando parte del tratamiento se efectúe fuera del mismo.

La interpretación del ámbito de aplicación de la ley de la autoridad de protección de datos, combina tres elementos: el domicilio del titular de los datos personales, como lo hace el estándar que trae el GDPR, una interpretación amplia de la expresión 'tratamiento' que comprende, por definición, la recolección de datos, y el hecho de que dicha recolección tiene lugar en territorio colombiano.

Más específicamente, la Delegatura para la Protección de Datos Personales de la SIC establece que:

> [B]uena parte del Tratamiento de los datos personales se realiza a través de internet lo que facilita, a modo de ejemplo, que en el territorio colombiano se recolecte la información y fuera del mismo los datos se procesen o usen. No obstante, ello no

> significa que por ese fenómeno tecnológico desaparezca la obligación de las organizaciones que operan globalmente de cumplir las normas locales, garantizar, de una manera efectiva y completa, el derecho a la protección de los datos personales y de respetar los derechos humanos.

Adicionalmente, la interpretación realizada por la SIC se ajusta al criterio que tiene la Corte Constitucional sobre la aplicación de la ley a empresas transnacionales. Por ejemplo, al analizar la constitucionalidad del Artículo 2.° de la Ley 1581 de 2012, la Corte indicó que dicha disposición se ajusta a la Constitución, en tanto:

> amplía el ámbito de protección a algunos tratamientos de datos personales que ocurren fuera del territorio nacional, en virtud del factor subjetivo. En un mundo globalizado en el que el flujo transfronterizo de datos es constante, la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de las fronteras.

Esta novedosa interpretación de la Delegatura es un avance en la protección de los datos personales de los colombianos en la era digital pues, alineada con la jurisprudencia constitucional, habilita la competencia de la autoridad de protección de datos para hacer rendir cuentas a las EMNBD que no se encuentran domiciliadas en Colombia. Sin embargo, no se puede perder de vista que las dos resoluciones reseñadas anteriormente (en los casos Facebook y Uber) son meros actos administrativos de carácter particular que no han sido sometidos al tamiz del control judicial de legalidad.

Sin embargo, la regla de la aplicación extraterritorial del derecho a la protección de datos personales parece respaldada por la Corte Constitucional colombiana, aunque, al resolver un tipo diferente de casos, se trata de casos relacionados con la moderación de contenidos publicados en redes sociales y en otras plataformas digitales (Twitter, Blogger, Youtube, etc.) en los cuales la Corte Constitucional ha avanzado la tesis de la legitimidad de las órdenes judiciales dirigidas a los administradores de dichas plataformas, orientadas a garantizar la tutela efectiva de los derechos fundamentales a la intimidad y al buen nombre. Recientemente,

en la Sentencia SU-420 de 2019, al resolver un caso que involucraba la posible responsabilidad de Google LLC y de Google Colombia por la publicación de un mensaje supuestamente deshonroso en un blog, alojado en la plataforma Blogger.com de su propiedad, consideró en obiter que los intermediarios eran responsables de forma 'subsidiaria', cuando no era posible conseguir la eliminación del contenido directamente con el editor de este. Sobre el punto consideró la Corte:

> Si bien las páginas que proveen herramientas para facilitar las publicaciones electrónicas no son los responsables de la infracción de los derechos a la honra o al buen nombre de las personas, al tener la única posibilidad de retirar el contenido vejatorio difundido en sus portales y, por tanto, ser los únicos actores con capacidad de detener el hecho vulneratorio mediante la eliminación de la publicación que perturbe los derechos fundamentales de una persona, en su calidad de administradores de la plataforma, son susceptibles de ser vinculados al proceso y destinatarios de una orden de amparo que pretenda la cesación del hecho constitutivo de transgresión invocada.

3.4. Capacidades de regulación, sanción, vigilancia y control de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio

A diferencia de lo que sucede en algunos países de la región (en donde no existe autoridad alguna) o en Estados Unidos (en donde legalmente no se le otorgan funciones de vigilancia a ninguna autoridad, pero *de facto* las asumió la Comisión Federal de Comercio), en Colombia existe una autoridad de protección de datos personales encargada de vigilar y garantizar que en el tratamiento de datos personales se respeten los principios, garantías y procedimientos previstos en la Ley 1581 de 2012. La Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio tiene, en virtud de la legislación colombiana, las siguientes funciones: 1) funciones de vigilancia y control, referidas a velar por el cumplimiento de la legislación de protección de datos, solicitar a los responsables de tratamiento para que demuestren que han implementado medidas para cumplir con las obligaciones de la Ley 1581 de 2012 y administrar el Registro Nacional Público de Bases de Datos y 2) funciones sancionatorias, entre las cuales se encuentra la de adelantar

investigaciones y, como resultado de ellas, ordenar medidas que hagan efectivo el derecho al habeas data, y la de requerir la colaboración de entidades internacionales cuando se afecten los derechos de los titulares fuera del territorio colombiano.

En la práctica, la Delegatura para la Protección de Datos Personales ha mejorado sus capacidades de sanción, vigilancia y control con el transcurso de los años. Por ejemplo, uno de los avances más visibles está en el personal especializado que trabaja en la Delegatura. En 2017, la entidad contaba con aproximadamente 30 funcionarios mientras que en 2020 el número total de trabajadores fue de 73. Esto quiere decir que en el término de tres años la entidad duplicó su fuerza de trabajo, lo cual le permite desarrollar mejor sus labores.

De hecho, los datos disponibles evidencian un cambio en las capacidades de vigilancia y control de la Delegatura en los últimos cuatro años. Según las estadísticas disponibles sobre el desempeño de la SIC, en 2016 la Delegatura tramitó alrededor de 6000 denuncias de *habeas data* y expidió casi 400 órdenes o multas. En 2019, la misma Delegatura —pero con el doble de personal— tramitó más de 12000 denuncias de *habeas data* y expidió casi 1000 órdenes o multas. Esto quiere decir que, de manera proporcional al aumento en su fuerza de trabajo, la SIC duplicó sus capacidades de sanción, vigilancia y control en materia de protección de datos personales.

Recientemente, la Delegatura ha enfocado parte de su trabajo al tratamiento de datos personales en la era digital. Entre 2018 y 2019, en el marco de la Red Iberoamericana de Protección de Datos, esta Delegatura lideró la expedición de guías sobre: 1) tratamiento de datos e Inteligencia Artificial, 2) tratamiento de datos para fines de comercio electrónico, 3) tratamiento de datos para fines de marketing y publicidad y 4) responsabilidad demostrada en las transferencias internacionales de datos personales. Estas guías, si bien no son instrumentos normativos vinculantes para quienes realizan tratamiento de datos personales, sí constituyen estándares de buenas prácticas a tener en cuenta.

El aumento en las capacidades de trabajo de la Delegatura se ha materializado en la expedición de varias decisiones sobre la protección de datos en la era digital. Tres de ellas merecen una breve mención.

La primera es la Resolución 74 828 de 2019. En este caso, la Delegatura decide confirmar la sanción impuesta a Rappi, una plataforma de intermediación de servicios de mensajería, por desconocer el principio

de libertad. En el caso, la Delegatura afirma la distinción entre la creación del usuario y la autorización para el tratamiento de datos personales y considera que:

> la creación de un usuario en la plataforma tecnológica no significa, *per se*, que [el titular] autorizó el tratamiento de sus datos personales. Al contrario, para poder crear dicho usuario es necesario obtener la autorización del mismo cuando para dicho efecto se utilicen datos personales.

En esta decisión, la Delegatura manda un mensaje claro a las EMNBD para que distingan los dos fenómenos y se abstengan de asimilar el hecho de aceptar los términos y condiciones, o dar *click* en el aviso de privacidad, con una declaración formal de autorización para el tratamiento de datos personales.

En la misma línea, la segunda decisión relevante es la Resolución 76 538 de 2019. En este caso, la compañía Asegúrate Fácil Ltda. informaba a sus usuarios digitales que al hacer *click* en el botón 'calcular valor', habilitado en su página web, se aceptaban las políticas de privacidad de la empresa y, por tanto, la autorización para el tratamiento de datos personales. Entonces, la Delegatura confirmó la sanción impuesta y estableció de manera clara que el hacer *click* en un botón, no relacionado con el tratamiento de datos personales, no era apropiado para otorgar un consentimiento válido. Sobre el punto indicó la Delegatura que "el silencio, las casillas 'premarcadas' por defecto y la inacción no constituyen consentimiento bajo la Ley 1581 de 2012".

La tercera, es la Resolución 54 265 de 2019 en donde la Delegatura consideró que utilizar la plataforma web ofrecida por Facebook Inc. para la recolección de datos, no exime al responsable del cumplimiento de la Ley 1581 de 2012 y de sus normas reglamentarias. En el caso, decidió conminar a la empresa Wikimujeres S.A.S. a respetar los derechos de los titulares de los datos personales que recolecta mediante un dominio vinculado con facebook.com.

3.5. Competencia frente a las EMNBD

La Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio tiene competencia sobre empresas colombianas y sobre empresas extranjeras a quienes les sea aplicable la ley de protección de datos. Sin embargo, en la práctica, la Delegatura ha

tenido dificultades para afirmar su autoridad sobre los responsables o encargados de tratamiento que no están domiciliados en Colombia. A pesar de los avances descritos en el apartado sobre el ámbito de aplicación de la Ley 1581 de 2012, a propósito de las Resoluciones sobre Facebook y Uber, estas decisiones fueron apeladas. Según Uber y Facebook, la regulación colombiana de datos personales no les es aplicable porque no están domiciliadas en el territorio colombiano y porque el tratamiento-análisis de la información personal lo adelantan fuera de Colombia.

Sin embargo, en el caso de Facebook, el 13 de febrero de 2020, mediante Resolución 4885 de 2020, el Superintendente Delegado para la Protección de Datos Personales resolvió el recurso de apelación interpuesto por dicha EMNBD. Entonces confirmó la decisión de primera instancia y reiteró que Facebook Colombia S.A.S. es una subsidiaria de Facebook Inc.; que el modelo de negocios de Facebook Colombia S.A.S. se basa en la recolección, uso y circulación de información que realiza Facebook Inc.; que Facebook Colombia S.A.S. realiza tratamiento de datos personales y que a dicho tratamiento le es aplicable la Constitución y la Ley colombianas. Esta decisión sienta la postura definitiva de la autoridad nacional de datos personales. En todo caso, a pesar de la importancia que tiene le resolución del caso Facebook, aún está por verse la capacidad que tendrá esta autoridad para lograr que las EMNBD, sin domicilio en Colombia, efectivamente rindan cuentas respecto del tratamiento de los datos personales de las personas domiciliadas en Colombia y sometidas a su jurisdicción.

Referencias

1DOC3 S.A.S. *Manual de políticas y procedimientos para la protección y tratamiento de datos personales.* Consultado junio 1, 2018. https://www.1doc3.com/web/politicas

Acsendo S.A.S. *Política de Protección de Datos Personales*. Consultado junio 1, 2018. https://www.acsendo.com/es/privacidad/

Alibaba Group. *Privacy Policy*. Consultado junio 1, 2018. http://rule.alibaba.com/rule/detail/2034.htm

Almacenes Éxito S.A. *Política manejo de información y datos personales de Almacenes Éxito S. A.* Consultado junio 1, 2018. https://www.grupoexito.com.co/files/Poltica_manejo_de_informacin_y_datos_personales_3.pdf

Amazon Inc. *Aviso de Privacidad.* Consultado junio 1, 2018. https://www.amazon.com/gp/help/customer/display.html?language=es_US&nodeId=468496

App Annie. *Top App Matrix*. 2017. Consultado junio 20, 2018. https://www.appannie.com/en/

Apple Inc. *Política de privacidad.* Consultado junio 1, 2018. https://www.apple.com/legal/privacy/es-la/

Bending Spoons S.p.A. *Privacy Policy.* Consultado junio 1, 2018. https://bendingspoons.com/privacy.html

Biko Development Inc. *Privacy Policy.* Consultado junio 1, 2018. https://bikoapp.com/policy.html

Cívico Digital S.A.S. *Políticas de Tratamiento de Datos Personales.* Consultado m junio 1, 2018. https://www.civico.com/politicas-de-privacidad

Concepto 14-218349-00003-0000 [Superintendencia de Industria y Comercio]. Noviembre 24 de 2014.

Concepto 14-218349-4-0 [Superintendencia de Industria y Comercio]. Marzo 3 de 2016.

Concepto 16-172268-00001-0000 [Superintendencia de Industria y Comercio]. Agosto 9 de 2016.

Corte Constitucional. Sentencia SU-420/19 12 de septiembre de 2019. M.P. José Fernando Reyes. https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm

Corte Constitucional de Colombia. Sentencia C-748 de 2011. (M.P. Jorge Ignacio Pretel: octubre 6 de 2008). http://legal.legis.com.co/document/Index?obra=jurcol&document=jurcol_c5d6d-39c403e0084e0430a0101510084

Deezer S.A. *Política de privacidad y cookies.* Consultado junio 1, 2018. https://www.deezer.com/legal/personal-datas

Donantes, Ricardo. "Qué es una startup". *Enterpreneur,* agosto 22, 2019. Consultado noviembre 24, 2019. https://www.entrepreneur. com/article/304376

Duety S.A.S. *Legal.* Consultado junio 1, 2018. https://blog.duety.co/legal/#privacidad

Easy Taxi Colombia S.A.S. *Aviso de Privacidad*. Consultado junio 1, 2018. http://www.easytaxi.com/co/terms-conditions/aviso-de-privacidad/

Egan, Erin. *Portabilidad de datos y privacidad*. Facebook. 2019. Consultado febrero 25, 2020. https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf

Facebook Inc. *Política de datos*. Consultado junio 1, 2018. https://www.facebook.com/privacy/explanation

Facebook Inc. *Política de privacidad de WhatsApp*. Consultado junio 1, 2018. https://www.whatsapp.com/legal?eea=0#privacy-policy

Fluvip S.A.S. *Política para la protección y el tratamiento de datos personales de Fluvip*. Consultado junio 1, 2018. http://www.fluvip.com/home_policy_for_the_protection?locale=es_CO

Google LLC. *Política de Privacidad de Google*. Consultado junio 1, 2018. https://policies.google.com/privacy?hl=es-US&gl=us

Grupo Aval Acciones y Valores S.A. *Política de privacidad y tratamiento de datos personales*. Consultado junio 1, 2018. https://www.grupoaval.com/wps/wcm/connect/grupo-aval/2c470a75-992f-4db3-a47b-a70da487464b/Politica-Tratamiento-Datos-Personales.pdf?MOD=AJPERES

Inversiones CMR S.A.A. *Política de privacidad y tratamiento de datos personales de Inversiones CMR S.A.S. ("Domicilios.com" o la "Compañía")*. Consultado junio 1, 2018. https://domicilios.com/pages/politica-de-privacidad.html

IoT Services Inc. *Privacy Policy*. Consultado junio 1, 2018. https://ubidots.com/privacy-policy/

Ley Estatutaria 1266 de 2018. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diciembre 31 de 2008. D.O. 47.219. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 18 de 2012. D.O. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Ley 599 de 2000. Por la cual se expide el Código Penal. Julio 24 de 2000. DO. 44.097. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

Match Group, LLC. *Nuestro compromiso con usted.* Consultado junio 1, 2018. https://www.gotinder.com/privacy?locale=es

Microsoft Corporation. *Declaración de privacidad de Microsoft*. Consultado junio 1, 2018. https://privacy.microsoft.com/es-mx/privacystatement#mainhowtoaccesscontrolyourdatamodule

Microsoft Corporation. *Política de privacidad LinkedIn*. Consultado junio 1, 2018. https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv

Netflix International B.V. *Declaración de Privacidad.* Consultado junio 1, 2018. https://help.netflix.com/legal/privacy

Newman Pont, Vivian y María Paula Ángel Arango. *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*. Bogotá: Dejusticia, 2019.

Rappi S.A.S. *Aviso de Privacidad.* Consultado junio 1, 2018. http://wordpress.rappi.com.br/terms-conditions/

Resolución 1321 [Superintendencia de Industria y Comercio]. Por la cual se imparten órdenes dentro de una actuación administrativa. Enero 24 de 2019. https://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

Resolución 21478 [Superintendencia de Industria y Comercio]. Por la cual se imparten órdenes dentro de una actuación administrativa. Junio 17 de 2019. https://www.sic.gov.co/sites/default/files/files/Noticias/2019/ORDEN%20%20UBER.pdf

Resolución 54265 [Superintendencia de Industria y Comercio]. Octubre 11 de 2019.

Resolución 74828 [Superintendencia de Industria y Comercio]. Por la cual se resuelve un recurso de apelación. Diciembre 17 de 2019. https://www.sic.gov.co/sites/default/files/boletin-juridico/Res%2074828%20del%2017XII2019%20Rappi.pdf

Resolución 76538 [Superintendencia de Industria y Comercio]. Diciembre 27 de 2019.

Seguros Generales Suramericana S.A. *Política de privacidad y tratamiento de datos personales.* Consultado junio 1, 2018. https://www.segurossura.com.co/Paginas/legal/politica-privacidad-datos.aspx

SIA Joom (Latvia). *Joom Privacy Policy.* Consultado junio 1, 2018. https://www.joom.com/es/privacy

Spotify AB. *Política de privacidad de Spotify.* Consultado junio 1, 2018. https://www.spotify.com/co/legal/privacy-policy/

Telmex Colombia S.A. *Política de tratamiento de la Información*. Consultado junio 1, 2018. https://www.claro.com.co/portal/recursos/co/legal-regulatorio/pdf/Politicas_Seguridad_Inf_Claro.pdf

Uber B.V. *Política de Privacidad*. Consultado junio 1, 2018. https://privacy.uber.com/policy

Urbanite Inc. *Privacy Policy*. Consultado junio 1, 2018. https://8fit.com/privacy/

Unilever N.V. *Aviso de Privacidad*. Sin fecha de última actualización. Consultado junio 1, 2018. https://www.unileverprivacypolicy.com/spanish/policy.aspx

Waze Mobile Limited. *Waze – Privacy Policy*. Consultado junio 1, 2018. https://www.waze.com/es-419/legal/privacy

RENDICIÓN DE CUENTAS DE LAS EMNBD EN MÉXICO

*Milan Trnka Osorio**

1. Selección de las EMNBD

En el presente documento serán analizadas las políticas de privacidad de 4 empresas con modelos de negocio basados en datos (EMNBD) que operan en México, siguiendo los estándares establecidos en el informe "Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital" (Newman y Ángel 2019).

Dentro de la categoría 'grandes empresas de internet', que agrupa a las cinco empresas comúnmente referidas con el acrónimo GAFAM (Google, Amazon, Facebook, Apple y Microsoft), se escogió a la empresa Amazon. Se eligió a Amazon, por sobre las demás grandes empresas que conforman el grupo de GAFAM, para abordar su aviso de privacidad por la presencia que tiene en el mercado mexicano. Fue en julio de 2015 que se anunció oficialmente la llegada de sus servicios a México mediante su página web (www.amazon.com.mx), considerado como el lanzamiento más ambicioso de la firma en 20 años (CNNExpansión 2015), México es el país de América Latina en el que Amazon tiene su más grande centro de distribución para la región (Milenio 2019).

Como empresa intermedia, considerando como tales a las empresas que, si bien no se encuentran en una etapa temprana para ser calificadas como *start-ups*, tampoco han alcanzado aún el nivel de consolidación de

* Abogado, Universidad Nacional Autónoma de México (UNAM). Oficial jurídico en R3D: Red en Defensa de los Derechos Digitales.

las grandes empresas de internet, se seleccionó a Snap Inc. y su producto Snapchat, que es una plataforma que ofrece servicios de redes sociales con creciente popularidad en México, según lo indica el ranking de la empresa de información y mercado de aplicaciones App Annie (https://www.appannie.com/en/) respecto de las aplicaciones más descargadas en la App Store y Google Play desde México.

Para a la categoría '*start-ups*', es decir, empresas que se definen por su temprana edad, escalabilidad y crecimiento exponencial, se eligió a la empresa Payclip S. de R. L. de C. V. y su producto Clip, que provee a los usuarios las herramientas para poder realizar cobros a tarjetas de crédito y débito desde su teléfono móvil o tablet. En su momento, la llegada de esta aplicación supuso un gran impulso a la innovación. Desde entonces, es considerada como una de las *start-ups* más exitosas del país, no solo por su practicidad y la facilidad de uso, sino también porque generó interés en los inversionistas, lo que provocó una gran llegada de capital desde Sillicon Valley a México (Küfner 2018).

Finalmente, como empresa establecida se buscó a la que fuera la más grande en el sector de telecomunicaciones y, para el caso mexicano, esta es Radio Móvil Dipsa S.A. de C.V., que es la empresa que ofrece el servicio de telefonía móvil más popular del país y por ende es el producto analizado: Telcel.

Al igual que en el Informe, para cada EMNBD habrá 4 categorías distintas de análisis para caracterizar su forma de operar: 1) fuente de datos, 2) tratamiento de datos, 3) finalidades del tratamiento y 4) relación con GAFAM. Posteriormente, se procederá a ofrecer un estudio de la preparación de régimen legal mexicano, así mismo se evaluará a la autoridad encargada de la protección de datos.

2. Caracterización de las formas de operar de las EMNBD

A partir de la revisión de las políticas de privacidad de los productos y servicios ofrecidos por las 4 empresas que hacen parte de la muestra, a continuación, se analiza la caracterización de su forma de operar, con base en las siguientes cuatro categorías de análisis: 1) fuente de datos, 2) tratamiento, 3) finalidades de tratamiento y 4) relación con GAFAM. La sistematización de este análisis puede ser consultado en el Anexo 1.

2.1. Fuente de datos

Tanto Amazon como Snapchat dividen en 3 categorías sus fuentes de datos: 1) datos proporcionados por el usuario/cliente, 2) información generada automáticamente como consecuencia de la prestación del servicio y que es recolectada con técnicas de *web tracking* y *crowdsourcing* y 3) la información que recaban de terceros. Sin embargo, mientras que Snapchat incluye distintas secciones relacionadas con su política de privacidad para hacer más comprensible y sencilla la lectura (Nuestros principios de privacidad, Tu privacidad explicada, Privacidad por producto, Cómo usamos tu información y un Informe de transparencia. Además, proporciona un enlace para tener contacto directo con el área encargada de la privacidad y una política especial para el uso de *cookies*), Amazon, por su parte, se limita a ofrecer un solo ejemplo por cada tipo de información que recaba mediante cada una de las fuentes. Concretamente, en los 5 párrafos que dedica a explicar la información que consigue, utiliza 5 veces la expresión 'por ejemplo' o similar (esto es un incumplimiento explícito al 22.° lineamiento de los avisos de privacidad)[1].

Payclip hace más bien referencia a la categoría de información que recaban en lugar de referirse a la fuente de la información. En este sentido, menciona que recaba de "manera enunciativa mas no limitativa", datos de identificación, informáticos, de geolocalización, de contacto (entre ellos, laborales, comerciales, financieros y patrimoniales) y datos de terceros. Payclip no proporciona una lista exhaustiva de los datos que recaba sino más bien presenta una lista ilustrativa de las diferentes categorías de información a las que pertenecen los datos recogidos. Debe señalarse la falta en la que está incurriendo aquí al no ser exhaustiva y precisa en cuanto a la información que obtiene y, en su lugar, ser vaga y

1 "**Vigésimo segundo**. El aviso de privacidad deberá indicar los datos personales que el responsable tratará para la consecución de las finalidades para las que los obtiene, tanto los que recaba personal o directamente del titular, como aquellos que obtiene indirectamente, por medio de fuentes de acceso público o transferencias, en términos del Artículo 15 de la Ley.
El responsable podrá cumplir con este contenido identificando los datos personales que trata o las categorías de los mismos.
El listado de datos personales o en su caso la mención de las categorías no deberá incluir frases inexactas, ambiguas o vagas, como 'entre otros datos personales' o 'por ejemplo'" (Estados Unidos Mexicanos 2013).

ambigua con expresiones como "de manera enunciativa mas no limitativa" y utilizando categorías genéricas para referirse a los datos recabados como consecuencia de la prestación del servicio. Esto es, nuevamente, un incumplimiento al 22.° lineamiento de los avisos de privacidad mencionado en el párrafo anterior. Y si bien es cierto que en su mismo aviso de privacidad refiere que no recaba datos sensibles, esto no puede ser absolutamente comprobado si no se señalan de manera específica los datos que se recaban.

Asimismo, cabe señalar que, por la propia naturaleza del servicio prestado, consistente en proveer a los usuarios las herramientas para poder realizar cobros a tarjetas de crédito y débito desde su teléfono móvil o tablet, el usuario de Clip manejará datos personales de los terceros a los que les preste el servicio o transfiera el bien que podrá cobrar con la aplicación. Y es en virtud de lo anterior que, al aceptar el aviso de privacidad, Clip se obliga a contar con su propio Aviso de Privacidad en el que se establezca que sus clientes le autorizan transferir sus datos personales y sensibles a su favor, con la finalidad de que pueda tratar tales datos para el cumplimiento de la prestación de servicios entre Clip y su cliente. Y el cliente se obliga a sacar en paz y a salvo a Clip en caso de un incumplimiento.

Radiomóvil Dipsa, por su parte, distingue entre los datos personales consecuencia del servicio (y dentro de estos se mencionan los datos de identificación y autenticación, de contacto, patrimoniales y/o financieros, fiscales, demográficos, de ubicación del dispositivo, de red y tráfico y sobre las preferencias del usuario) y los datos personales sensibles, los cuales, según refiere en su aviso de privacidad, son "datos biométricos referentes a sus huellas dactilares con la finalidad de identificarle y acreditar su identidad para la provisión de los Servicios y futuras operaciones que usted realice ante Telcel" (Telcel 2019). Asimismo, refiere a la recolección de datos por fuentes indirectas, ya sea por medio de comunicaciones con empresas afiliadas o con terceros con los que Telcel tenga celebrados acuerdos comerciales o por fuentes de acceso público (incluyendo las redes sociales). Por último, se refiere a los datos de terceros que pudiera recabar y que obtendrá del usuario, pues en algunos casos es necesario tener un aval para poder tener acceso a un bien o servicio.

2.2. Tratamiento

Tal y como fue el caso para las EMNBD analizadas en el Informe, los tratamientos de datos personales por las EMNBD aquí analizadas también tienden hacia la uniformidad, centrándose en las mismas dos actividades: recolección y análisis. Por cuanto hace a la recolección, las herramientas utilizadas son comunes a las 4 empresas:

- *Cookies* (propias y de terceros): son pequeños elementos de información que se almacenan en el dispositivo para ayudar a los sitios web y aplicaciones móviles a recordar cosas específicas sobre el usuario cuando este vuelve a visitar el sitio.
  - SNAP Inc.: para proteger datos del usuario, tener conocimientos sobre las características más populares de la aplicación y/o el número de visitas a la página y ofrecer servicios más personalizados. Dividen las *cookies* utilizadas en 4 categorías: 1) necesarias (para detectar riesgos de seguridad y corregirlos); 2) preferencias (recordar ajustes y preferencias, mejorar la experiencia del usuario); 3) desempeño (información sobre el uso del sitio web con la finalidad de monitorear y mejorar el desempeño); y 4) mercadotecnia (ofrecer publicidad, anuncios y campañas publicitarias especializadas y dirigidas a los usuarios según su perfil y sus intereses).
  - Amazon: permitir a los usuarios tener acceso a características y anuncios del servicio personalizados.
  - Payclip: monitorear el comportamiento como usuario de internet para brindar un mejor servicio y experiencia de usuario, así como ofrecerle nuevos productos y servicios basados en sus preferencias.
  - Telcel: no especifica el uso que le da a la información recabada por medio de este método.
- Web beacons / Etiquetas de píxel: tipo de tecnología presente en un sitio web o en el interior del cuerpo de un correo electrónico, permite realizar un seguimiento de ciertas actividades.
- Almacenamiento web: tecnología de almacenamiento local que permite que los sitios web almacenen datos en el navegador de un dispositivo.

- URL: enlaces personalizados que le ayudan a las empresas a comprender de dónde viene el tráfico de sus páginas web.
- Identificadores únicos de aplicaciones y dispositivos: cadena de caracteres que se puede utilizar para identificar de forma exclusiva un navegador, una aplicación o un dispositivo.
- Sensores: mecanismo interno de los dispositivos que los capacita para medir y detectar acciones o estímulos externos y actuar en consecuencia (acelerómetro, giroscopio, barómetro, magnetómetro, sensor de proximidad, sensor de luz, termómetro, sensor de ritmo cardíaco, podómetro, lector de huellas, etc.).

En relación con las *cookies* como medio para recopilar información, es destacable el hecho de que Snapchat cuenta con su propia "Política de *cookies*" (que entró en vigor el 15 de enero del 2019) y ofrece al usuario de esta plataforma más información específicamente sobre tecnologías como *cookies*, almacenamiento web y los identificadores asociados con el dispositivo. Asimismo, clasifica las *cookies* según el criterio por el cual las utilizan: 1) Necesarias, 2) Preferencias, 3) Desempeño, 4) Mercadotecnia y ofrece una pequeña guía al usuario sobre cómo desactivarlas tanto en el navegador como en su propio dispositivo móvil.

Ahora bien, en cuanto al análisis de los datos recabados, este se divide en dos vertientes: la primera busca personalizar el servicio y segmentar a los usuarios en grupos con intereses y conexiones comunes (estas pueden ser desde los contactos en la agenda, los lugares que ha visitado, los anuncios que ha visto o los productos sobre los que haya dado click), es decir, un análisis de tipo descriptivo. Por otro lado, se hace un análisis prescriptivo encaminado a mejorar la experiencia de uso para conocer las características más populares del producto o servicio. No se especifica en ninguna de las 4 políticas de privacidad las tecnologías o los métodos utilizados para llevar a cabo estos análisis.

Respecto a este punto, en la política de privacidad de Telcel se refiere, por ejemplo, que entre las finalidades que se les darán a los datos recabados está la de:

> realizar tratamientos de técnicas de análisis masivo de datos para actividades de perfilamiento a partir de combinar información facilitada por usted, la obtenida de fuentes de acceso público, incluyendo redes sociales, y aquella información que se pueda

> inferir u obtener como resultado de la aplicación de diversas tecnologías de análisis de datos (Telcel 2019).

Si bien sí hay una mención sobre tecnología de análisis, no se especifica en qué consiste. Por otra parte, Payclip señala en su política de privacidad que una de sus finalidades primarias es la "creación, integración, análisis, actualización y conservación de su expediente", nuevamente sin especificar la tecnología utilizada para cumplir con este fin.

2.3. Finalidad

En las políticas de privacidad de cada una de las EMNBD analizadas en el presente estudio, se mencionan finalidades similares para los datos recabados. De manera general, estas incluyen acreditar la identidad del usuario, mejorar la seguridad, personalizar los servicios y los anuncios, generación de perfiles y creación, actualización, análisis y conservación de expedientes, análisis y estudios de prospección comercial, compartir con terceros, etc.

Para el caso de Amazon, como ya fue mencionado con anterioridad, esta EMNBD no proporciona una lista exhaustiva de las fuentes de las cuales recolecta la información de sus usuarios, sino que más bien únicamente proporciona ejemplos ilustrativos del 'tipo' de fuente de la que puede sacar la información, ocurre algo similar en su apartado de finalidad. Nuevamente, esto es un incumplimiento a los lineamientos sobre avisos de privacidad que explícitamente prohíben la ambigüedad o generalidades para describir los procesos de recolección y tratamiento que dan a los datos personales.

Telcel es más preciso al elaborar una lista puntual de las finalidades principales en que pueden derivar los datos recolectados, para esto se mencionan los mismos usos generales que en otras políticas similares como son verificar la identidad, contactar al usuario, monitorear los usos de los productos por parte de los clientes para mejorarlos y personalizarlos, dar cumplimiento a la obligación de cooperar con instancias de seguridad y justicia (finalidad específica de Telcel por la naturaleza del servicio) y planear y llevar a cabo procedimientos de disociación para generar audiencias segregadas para que terceros o socios comerciales puedan ofrecer sus productos y servicios. Por otro lado, por lo que hace a las finalidades secundarias del tratamiento (que el usuario tiene la

opción de solicitar que sus datos no sean utilizados para estas), señala que se usarán los datos para informar al usuario sobre promociones, nuevos lanzamientos u ofertas de acuerdo con el perfil y hábitos de consumo que fueron generados.

Payclip divide también las finalidades de los datos recolectados entre primarias y secundarias, siendo las primeras aquellas esenciales y necesarias para poder proporcionar el servicio, y las segundas aquellas en que el usuario puede solicitar que no se usen sus datos. En este sentido, refiere que son finalidades primarias la celebración de contratos para formalizar la prestación del servicio, el envío y recepción de los lectores 'clip', pago de las transacciones y la emisión y envío de documentos que acrediten la transacción (facturas, recibos).

Finalmente, Snapchat tiene, además de su política de privacidad, una sección especial para explicar al usuario cómo se utiliza su información. En esta describe que la primera y más importante finalidad es el desarrollo de la aplicación. Esto quiere decir conocer las características más usadas y populares para que sirvan como referencia para innovaciones futuras. Asimismo, usa la información para personalizar el servicio y los anuncios publicitarios.

2.4. Relación con GAFAM

Ninguna de las 3 empresas estudiadas menciona de forma explícita alguna relación con empresas del grupo GAFAM. Sin embargo, sí existen entre estas y aquellas algunas conexiones que es necesario referir. Para empezar, tanto Clip como Telcel utilizan 'botones sociales', aquellos enlaces incluidos en las páginas web para compartir información de manera directa en las distintas redes sociales, los botones hacen de nexo entre una página web y la otra. Los más comunes son aquellos ligados a las grandes empresas, como el botón 'me gusta' de Facebook, el 'Tweet' de Twitter o el '+1' de Google+.

Snapchat tiene sus servicios ligados a los mapas de Google y de Apple y tiene la cámara del dispositivo vinculada con Amazon. Sobre estos puntos, las políticas de privacidad son muy opacas y carecen de claridad. Como ya se dijo, no hay ninguna referencia o mención directa y específica de la relación que tienen con grandes empresas, sin embargo, de manera práctica es posible ver como sí están ligadas.

3. Evaluación del nivel de preparación del régimen jurídico de protección de datos personales para abordar nuevas dinámicas propias de la era digital

A la luz de la forma de operar de las empresas aquí estudiadas, se pasa ahora a establecer el nivel de preparación del régimen legal mexicano y de las autoridades competentes para enfrentar los riesgos, y llamar a estas empresas a rendir cuentas en cuanto al tratamiento de datos personales recabados en México.

3.1. Alcance del régimen de protección de datos

En México, el derecho a la protección de datos personales es un derecho humano, previsto en el Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Como leyes reglamentarias de dicho precepto, se emitieron la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Pertinente para el presente análisis, a continuación, nos centraremos en la LFPDPPP.

El ámbito de aplicación de la LFPDPPP comprende todas aquellas personas físicas o morales de carácter privado que lleven a cabo actividades de tratamiento de datos personales, esto incluye a personas responsables del manejo de datos personales que no se encuentren físicamente en territorio mexicano.

El reglamento de la LFPDPPP refiere en su Artículo 4 que la legislación es aplicable aun cuando el responsable no esté establecido en territorio mexicano, pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional, y cuando el responsable no esté establecido en territorio mexicano pero utilice medios situados en dicho territorio, salvo que tales

medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento (fracciones III y IV).

Están exceptuadas de estas disposiciones: 1) las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables; y 2) las personas que lleven a cabo la recolección y almacenamiento de datos personales para uso exclusivamente personal y sin fines de divulgación o utilización comercial (Artículo 2). En este sentido, por 'tratamiento' deberá entenderse toda "obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio" (Artículo 3, fracc. XVIII). Asimismo, el 'uso' deberá interpretarse como "cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales" (Artículo 3, fracc. XVIII).

Profundizando en el alcance de protección conferida por la LFPDPPP, de acuerdo con su Artículo 6.°, cualquier tratamiento de datos personales deberá estar regido por los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (Artículo 6).

La ley establece de manera expresa, entre lo más destacable, que la obtención de datos personales no deberá hacerse mediante maneras engañosas o fraudulentas y que se presume que existe la expectativa razonable de privacidad, la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por ellas (Artículo 7).

Asimismo, la ley establece que, tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, por medio de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca y que no podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de estas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado (Artículo 7).

De conformidad con lo anterior, si bien podría argumentarse que el régimen de protección de datos personales en México es de los más sólidos, a comparación de los otros existentes en la región, lo cierto es que atendiendo los cada vez más cambiantes e inminentes avances tecnológicos, el ámbito de protección existente en la materia resulta

insuficiente para enfrentar los potenciales riesgos o vulnerabilidades que de ello deriven.

Por tanto, tomando como ejemplo el Reglamento Europeo de Protección de Datos Personales (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, en adelante el Reglamento) como el California Consumer Privacy Act[2] (en adelante el CCPA), dado su ámbito de protección y de la forma en que prevén cuestiones propias al entorno digital, en adelante se abordan aquellos aspectos aún no previstos por la legislación mexicana y cuya incorporación amerita ser considerada.

3.1.1. Lo que no está regulado y debe regularse

La LFPDPPP establece en su Artículo 3, fracción V, una definición de 'datos personales' bastante parecida a la prevista tanto por el Reglamento como por el CCPA, entendiendo estos como "cualquier información concerniente a una persona física identificada o identificable".

3.1.2. Datos sensibles inferidos

Por su parte, como 'dato personal sensible' la LFPDPPP reconoce a aquellos "datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este". En particular, aquellos que "puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual" (Artículo 3, fracc. VI).

No obstante, la LFPDPPP no ofrece suficiente claridad respecto de si las definiciones anteriores incluyen los datos inferidos a partir de otros datos, en particular, la inferencia de categorías sensibles a partir de la agregación de datos no sensibles. Si bien la CCPA tampoco hace referencia a los datos inferidos sensibles, el literal (o) de la sección 1798140, sí hace mención explícita de las inferencias extraídas de diversas categorías de datos.

3.1.3. Dirección IP

Contrario a los desarrollos existentes en el derecho europeo (Newman y Ángel 2019) y a la mención explícita en la CCPA, la LFPDPPP no ofrece

---

2 Assembly Bill No. 375, Chapter 55, an act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy, approved by Governor on June 28, 2018.

protección explícita de identificadores en línea, como las direcciones IP, lo cual genera incertidumbre jurídica y falta de homogeneidad en el tratamiento de estos datos por parte de las EMNBD. Esta práctica, que a primera vista puede parecer relativamente inofensiva, es en realidad una invasión a la privacidad de los usuarios en el sentido de que las direcciones IP permiten conocer, con un alto grado de exactitud, la ubicación desde donde un equipo accede a la red y, por tanto, la dirección IP podría ser considerada como un dato personal en caso de que el proveedor posea todos los datos necesarios para asociar esa IP a una persona concreta y de esta manera saber dónde ha estado y los sitios que ha visitado.

3.1.4. Tratamiento automatizado o elaboración de perfiles

En el mismo sentido, la LFPDPPP se queda corta y no ofrece protección explícita respecto de toda forma de tratamiento automatizado de datos personales consistente en su utilización para evaluar determinados aspectos personales de una persona física, en particular, para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de una persona física. Asimismo, a diferencia del Reglamento, la LFPDPPP carece de un ámbito de protección para el cifrado de datos (regulado por el Artículo 83 del Reglamento) así como para el tratamiento de datos personales sistemático o a gran escala (previsto por el Artículo 91 del Reglamento).

Adicionalmente, el Estado Mexicano incluso se encuentra en incumplimiento de su obligación de emitir la legislación reglamentaria relevante. En efecto, el Artículo 42 de la LFPDPPP establece que, en lo que concierne a las bases de datos de comercio, la Secretaría de Economía deberá emitir regulación aplicable a bases de datos automatizadas o que formen parte de un proceso de automatización. No obstante, a la fecha de redacción del presente informe tal regulación no ha sido expedida.

Regular con mayor profundidad los derechos de los titulares frente al tratamiento automatizado de sus datos personales resulta particularmente relevante para México, considerando que el país se ha visto involucrado en escándalos como el de Cambridge Analytica, extinta compañía privada con sede en Londres que se ha reportado que "usa el análisis de datos para desarrollar campañas para marcas y políticos que buscan cambiar el comportamiento de la audiencia" (BBC Mundo, 2018). A partir del pasado 19 de marzo de 2019, diversas notas periodísticas

revelaron que dicha compañía adquirió, de manera presumiblemente ilegítima, los datos personales de alrededor de 50 millones de personas por medio de una aplicación de Facebook llamada "*thisisyourdigitallife*" (Cabrera 2017, Murata, San Martín, Linares 2018).

La obtención de dichos datos se presume ilegítima en función de que, contrario a lo manifestado por Facebook, la mayoría de los usuarios que se vieron afectados no otorgaron un consentimiento informado para que sus datos fueran explotados de esa manera ni mucho menos para esas finalidades. Los usuarios desconocían que mediante la instalación de la aplicación en cuestión estaban facilitando el acceso de esta a los rasgos de su personalidad, salud mental, orientación sexual, preferencia política, historial de abuso de sustancias y demás información que pudieran revelar las páginas a las que le hubieran dado "me gusta" en la red social (Tufekci 2017).

Estos datos constituyen datos personales sensibles, de conformidad con el Artículo 3 de la LFPDPPP, no obstante su tratamiento automatizado y/o la elaboración de perfiles de sus titulares son cuestiones que aún no se encuentran previstas explícitamente por la ley.

Sin embargo, a la fecha no existe evidencia o información pública disponible de que la autoridad competente en la materia, el Instituto Nacional de Transparencia y Acceso a la Información Pública (INAI), haya sancionado esta práctica en el país, o cuando menos, implementado efectivamente el proceso de verificación correspondiente para la debida investigación de este caso. Aunado a ello, tampoco existe evidencia o información pública disponible que demuestre que se están desplegando esfuerzos para ampliar el ámbito de protección de la LFPDPPP al tratamiento automatizado de datos personales y/o a la elaboración de perfiles de las y los usuarios sin su consentimiento ni, peor aún, sin su conocimiento, situación que claramente vulnera el derecho de protección de datos personales.

3.1.5. Datos biométricos

Además de lo anterior, a diferencia del Reglamento y del CCPA, la LFPDPPP no incorpora expresamente entre su definición de datos personales sensibles aquellos relativos a los datos biométricos. Regular plena y detalladamente su tratamiento resulta crucial considerando el grado de sensibilidad, de identificación única de un individuo, así como del nivel de información que se puede desprender de este por dicha categoría de

datos, ya que entre estos se encuentran, por ejemplo, aquellos obtenidos a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Para demostrar la importancia de regular el tratamiento de este tipo de datos, el CCPA incluso desarrolla este concepto encuadrando en él aquella información "fisiológica, biológica o características del comportamiento de un individuo incluyendo información relativa a su ADN (ácido desoxirribonucleico) que pueda usarse de manera aislada o entre sí o en combinación con otros datos de identificación, para establecer la identidad de un individuo" (State of California 2018, Assembly Bill No. 375, section 1798.140, para (b)).

La información biométrica se incluye, pero no se limita a imágenes del iris, retina, huella digital, cara, mano, palma de la mano, patrones de las venas, así como grabaciones de voz, de las cuales se pueda extraer una plantilla de identificación, tales como un "*faceprint*", "*minutiae template*", así como patrones o ritmos de tecleado, forma de caminar, sueño, salud o información de ejercicio físico que contengan datos de identificación.

Partiendo de este contexto, resulta crucial mencionar que es particularmente preocupante el potencial uso de la biometría en consonancia con sistemas de vigilancia masiva que permitan identificar de forma factible los datos recolectados por los sensores que nos rodean. De dichos sistemas es posible derivar patrones biométricos que, combinados con los datos personales que suelen recabarse de nosotros diariamente, pueden dar pie a bases de datos que comprometan seriamente el anonimato (Chayka 2015), así como el ejercicio de otros derechos.

Al respecto, el Consejo de Derechos Humanos de las Naciones Unidas ha señalado que generalmente los datos que son recogidos con propósitos específicos terminan siendo usados para la vigilancia masiva y, sin las adecuadas salvaguardas procesales y legales, y, además, perjudican los derechos humanos (UNHR 2014). Por tanto, es fundamental que la LFPDPPP, o su interpretación por parte de la autoridad de protección de datos personales, permita derivar reglas claras y delimitadas para el tratamiento de este tipo de datos personales.

3.1.6. Otros datos personales relevantes propios del entorno digital

Además de lo anterior, tomando como punto de partida el CCPA, la LFPDPPP carece de una regulación que maneje como tratamiento de dato personal diversas categorías de datos relevantes respecto del entorno digital.

3.1.7. Información comercial

Esta incluye registros de propiedad, productos o servicios adquiridos, obtenidos o considerados o cualquier otra información de historial o tendencias de compras o consumo. Esta información es de particular importancia para las EMNBD que comercializan bienes y servicios, pues es la que les permite llevar a cabo análisis más profundos con base en los hábitos de sus usuarios, concretamente permite la creación de perfiles y la segregación de usuarios según intereses comunes. A partir de esta información, las empresas pueden dirigir publicidades específicas a los usuarios, según su comportamiento en línea y asimismo determinar las conductas de estos.

3.1.8. Información de actividad en internet o en cualquier otra red electrónica

Esta categoría de información suele entenderse como, de manera enunciativa más no limitativa, el historial de navegación, historial de búsquedas e información relativa a la interacción de un consumidor con un sitio web, app o publicidad en línea, entre otros. La necesidad de que la LFPDPPP reconozca expresamente y regule el tratamiento de este tipo de información como dato personal encuentra su sustento en que de una recopilación y análisis de esta es posible inferir rasgos propios de la personalidad, estado de ánimo, estado de salud, orientación sexual, preferencias ideológicas, religiosas y políticas, y demás información de naturaleza altamente sensible, que permite la creación de perfiles que además suelen comercializarse o transferirse a terceros, la mayoría de las veces sin que medie conocimiento ni el consentimiento para ello de las y los usuarios, en absoluta violación de su derecho a la autodeterminación informativa, entre otros.

3.1.9. Localización geográfica

El reconocimiento de los datos de localización de una persona como datos personales resulta de particular importancia, sobre todo considerando que, de acuerdo con la Ley Federal de Telecomunicaciones y Radiodifusión, específicamente los Artículos 189 y 190, las empresas de telecomunicaciones están obligadas a recolectar, almacenar y proporcionar dicha información, incluso en tiempo real, a las autoridades competentes cuando estas se las requieran. No obstante, la protección jurídica de esta información ha sido deficiente, como lo demuestra la evidencia, basada en información pública, de que el acceso a este tipo de datos por parte de autoridades no facultadas para llevar a cabo este tipo de requerimientos ha sido frecuente (R3D 2018).

Incluso, se ha identificado que una de las empresas con el mayor número de usuarios de telecomunicaciones en el país, Telcel, ha proporcionado dicha información el 100 % de las veces que le fue requerida, sin haber llevado a cabo un análisis de la procedencia y legalidad de la solicitud respectiva (R3D 2018). Esto es de crucial importancia considerando que, como ya se mencionó, los datos que revela la localización geográfica constituyen datos altamente sensibles de una persona. En este sentido, el Grupo de Trabajo sobre Protección de Datos Establecido por el Artículo 29 de la Directiva 95/46/CE del Parlamento Europeo, mediante el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, claramente reconoce que los datos de localización revelan una gran cantidad de información sensible:

> Los dispositivos móviles inteligentes están muy estrechamente vinculados a las personas porque la mayoría de ellas tienden a mantener su dispositivo móvil muy cerca de ellas, en el bolsillo, en el bolso o sobre la mesilla de noche […]
>
> Esto permite a los proveedores de servicios de geolocalización disponer de una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un periodo de inactividad nocturna, puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. […] Un modelo de comportamiento también podría incluir categorías especiales de datos, por ejemplo visitas a hospitales y lugares de culto, presencia en actos políticos o en otros lugares específicos que, verbigracia,

> revelen datos sobre la vida sexual. Estos perfiles pueden ser utilizados para tomar decisiones que afecten significativamente a su propietario.

No obstante lo anterior, la LFPDPPP o cualquier otra legislación vigente en el país, así como su interpretación por parte de los órganos competentes, no definen cuestiones como el procedimiento a seguir para obtener este tipo de dato personal, ni lo reconocen como tal, ni regulan el tratamiento que deberá darse a los datos de localización obtenidos, ni las salvaguardas necesarias para detectar e impedir el abuso de la medida de vigilancia.

Lo anterior contraviene lo señalado por la Suprema Corte de Justicia de la Nación (SCJN) en su resolución de la Acción de Inconstitucionalidad 32/2012, mediante la cual decidió que la localización geográfica en tiempo real de equipos de comunicación móvil solamente podía considerarse constitucional si, *inter alia* limitaba su uso a situaciones excepcionales para la investigación de delitos particularmente graves definidos en la ley.

3.2. Lo que está inadecuadamente regulado

De manera similar al Reglamento Europeo, la LFPDPPP reconoce a los titulares la facultad de ejercer los siguientes derechos:

> Artículo 23.- Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento.
>
> Artículo 24.- El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos.
>
> Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales (Artículo 26: excepciones).
>
> Artículo 27.- El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular.

Como se mencionó anteriormente, si bien podría argumentarse que la legislación mexicana en materia de protección de datos personales es de las más sólidas de la región, lo cierto es que su ámbito de protección y los derechos que confiere a los titulares de datos personales siguen

siendo bastantes acotados para mitigar, reaccionar o resarcir posibles daños o vulnerabilidades propias del entorno digital y de los avances tecnológicos en este sentido. Si se toma como marco de referencia el Reglamento Europeo y el CCPA, es posible constatar algunas deficiencias normativas en cuanto a la pretensión de protección efectiva ofrecida por la LFPDPPP. Entre las cuales se encuentran:

- *Derecho a la portabilidad de los datos*, es decir, el derecho a recibir los datos personales que le incumban al titular, 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 sin que lo impida el responsable al que se los hubiera facilitado.
- *Derecho de oposición al tratamiento de datos personales con finalidades de mercadotecnia directa,* incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.
- *Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado*, incluida la elaboración de perfiles, que produzca efectos jurídicos para el titular o le afecte significativamente de modo similar.
- *Derecho a la reparación del daño*, ya sea de naturaleza económica o cualquier otra que se estime pertinente. La LFPDPPP aún no reconoce el derecho de los titulares a que el responsable del tratamiento de sus datos personales les pague una indemnización por los daños y perjuicios, materiales o inmateriales, que les genere en virtud de violaciones a sus obligaciones en la materia. En este sentido, tomando como base el CCPA, la LFPDPPP debería establecer que cualquier consumidor tendrá acceso, como mínimo, a la reparación por los daños y perjuicios que se le ocasionen cuando su información no cifrada o no reservada sea sujeta de acceso no autorizado, filtración, robo o divulgación debido a que la empresa incumple con su obligación de implementar y mantener medidas y prácticas de seguridad necesarias para proteger la información de acuerdo con su propia naturaleza. Para determinar el monto de la reparación del daño aplicable la LFPDPPP, también debería prever que el tribunal competente considere, por ejemplo, la naturaleza y gravedad de la conducta incurrida, el número de violaciones en este sentido,

la persistencia de la conducta, su duración, la voluntad detrás del actuar del sujeto activo, así como su número de bienes, grado responsabilidad y valor neto.

- *Derecho a ser representado por una entidad, organización o asociación sin ánimo de lucro.* La LFPDPPP tampoco contempla explícitamente que una entidad, organización o asociación sin ánimo de lucro debidamente constituida, con fines de interés público y de protección de derechos y libertades, pueda presentar, en nombre de los titulares de datos personales, la reclamación correspondiente o ejercer los derechos que le son conferidos por la misma ley. Asimismo, existen múltiples obstáculos para utilizar la figura de "acciones colectivas" contemplada en el Código Federal de Procedimientos Civiles para el caso de violaciones al derecho de protección de datos personales.
- *Derecho de exclusión (opt out).* En México tampoco se ha otorgado a los consumidores el derecho a oponerse, en cualquier momento, a que sus datos personales no sean comercializados a terceros por parte de aquellas empresas que hagan de eso su eje de negocio.
- *Derecho de inclusión (opt in) (aplicable a menores de edad).* Tampoco se ha regulado propiamente el tratamiento que deberá otorgarse por parte de una empresa o negocio a los datos de un consumidor que es menor de edad, cuando este consista en la explotación comercial de estos; entendiendo que, de acuerdo con los estándares internacionales en la materia, tal cuestión deberá estar prohibida a menos que el consumidor cuente con el consentimiento explícito de sus padres o de quien ejerza sobre ellos la patria potestad y sea mayor de 13 años de edad.
- *Notificación por vulneración.* Además de todo lo anterior, resulta de suma importancia que la LFPDPPP reconozca el derecho de los titulares a recibir una notificación por vulneración cuando sus datos personales hayan sido vulnerados o comprometidos. Notoriamente, tanto el Reglamento como el CCPA reconocen esta obligación por parte de los responsables del tratamiento.
- Transferencias transfronterizas de datos personales: en el mismo sentido, la LFPDPPP, a diferencia del Reglamento, carece de una provisión que establezca que las transferencias transfronterizas de datos personales de titulares que se encuentren en el país podrán

realizarse única y exclusivamente si el tercer país u organización internacional receptor cumplen con las condiciones establecidas por la misma ley, garantizando un nivel de protección adecuado y/o otorgando las garantías pertinentes para ello.

Esta cuestión también resulta de particular interés, tomando en cuenta la creciente tendencia y/o presión internacional para que los Estados adopten tratados bilaterales o multilaterales de asistencia mutua internacional para proporcionar la información personal de sus ciudadanos o habitantes. Si México quiere ser reconocido como un país cuyo nivel de protección sea suficiente para ameritar ser receptor de la información en cuestión, deberá exigir el mismo nivel de protección de regreso.

Una legislación robusta que tome en cuenta los aspectos mencionados con anterioridad permitiría atender de mejor manera los problemas que derivan de las prácticas negativas de las EMNBD aquí estudiadas. De esta manera, incluir en la legislación nuevas categorías de información recabada y considerarlas como datos personales englobándolas en una definición amplia de estos obligaría a las empresas a ser más precisas al señalar los datos recabados, pues podrían encuadrarlos dentro de las definiciones legales proporcionadas por la ley. Asimismo, se pueden esclarecer algunas cuestiones, como lo referente a los datos sensibles inferidos y al tratamiento automatizado y la elaboración de perfiles.

3.3. Consideraciones adicionales que deberían regularse

3.3.1. Esquemas de mejores prácticas

La LFPDPPP debería promover la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos orientados a demostrar que el responsable cuenta con las garantías adecuadas para la protección y transferencia de datos personales.

3.3.2. Registro de las actividades de tratamiento

Asimismo, cada responsable deberá llevar registro de las actividades de tratamiento efectuadas bajo su responsabilidad. El Reglamento enlista aquella información que el registro deberá contener, misma que incluye las transferencias de datos que se realicen a otro país u organización internacional (Artículo 30).

3.3.3. Actualización de categorías de datos personales

Tomando como ejemplo el CCPA, deberían adoptarse las regulaciones necesarias para actualizar la protección de datos personales a aquellas categorías de datos adicionales que deriven de cambios en la tecnología, en sus prácticas de recolección o en obstáculos para su implementación.

3.3.4. Regulación del derecho de cancelación de datos personales para su venta (right to opt-out)

También sería pertinente que la LFPDPPP establezca reglas y procedimientos para facilitar la solicitud de un consumidor para ejercer el derecho de cancelación respecto de la venta de sus datos personales. De igual forma, para regular que las empresas efectivamente garanticen los derechos de los consumidores para ejercer la cancelación respecto de la venta de sus datos personales.

3.3.5. Conciliación del derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información

Tanto el Reglamento como el CCPA hacen mención expresa de que el derecho a la protección de datos personales deberá ponderarse frente al derecho a la libertad de expresión y de información. Dado el nivel de interdependencia de ambos derechos, así como de la importancia de que exista una armonización entre estos, ya que por su propia naturaleza es por demás común que entren en conflicto sin que exista aun el conocimiento suficiente por parte de los legisladores como de los órganos impartidores de justicia para hacerlos coexistir de la manera menos lesiva posible, la LFPDPPP debería a su vez incorporar este principio.

3.4. Ámbito de aplicación territorial de la ley de protección de datos

La LFPDPPP no hace mención respecto de su ámbito territorial de aplicación. No obstante lo anterior, el Reglamento de la LFPDPPP desarrolla en su Artículo 4 dicho ámbito territorial de aplicación, aunque de manera sumamente acotada.

Dicho artículo señala que la obligatoriedad del cumplimiento de la normatividad mexicana en la materia dependerá de los siguientes supuestos:

- El tratamiento se lleve a cabo en un establecimiento del responsable ubicado en territorio mexicano.
- El tratamiento sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano.
- El responsable no esté establecido en territorio mexicano, pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional.
- El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento.

Los anteriores supuestos no ofrecen claridad respecto de la aplicabilidad de las normas de protección de datos personales en México a empresas que ofrecen servicios en el entorno digital ubicadas en el extranjero. Derivado de lo anterior, en la práctica, la propia interpretación del INAI[3] ha excluido de su competencia cualquier consideración relacionada al tratamiento de datos personales realizado por empresas de internet como YouTube o Google, alegando una falta de competencia territorial (El Informador 2017).

4. Evaluación de las capacidades de las Autoridades de Protección de Datos para hacer rendir cuentas a las EMNBD

El Artículo 6.°, apartado A, inciso VIII de la Constitución de México dispone la existencia de un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados. Este organismo es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el

3 Resolución del INAI al expediente número PPD 0094/14 de fecha 26 de enero de 2015.

cual está conformado por siete personas comisionadas, nombradas por el Senado de la República.

La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), relativa al sector privado, establece las facultades del INAI en relación con las actividades de tratamiento de datos personales de las EMNBD.

La LFPDPPP contempla varios mecanismos para garantizar el derecho a la protección de datos personales. En primer lugar, la ley reconoce los derechos de solicitar a una empresa el acceso, rectificación, cancelación y oposición (derechos ARCO), respecto de los datos personales que le conciernen. Ante cualquier inconformidad con la respuesta otorgada por el particular, la ley contempla el Procedimiento de Protección de Derechos (PPD), el cual debe interponerse ante el INAI, este último tiene la facultad de confirmar, modificar o revocar la respuesta otorgada por la empresa al solicitante.

Las resoluciones del INAI respecto de los PPD son impugnables mediante el juicio de nulidad ante el Tribunal Federal de Justicia Administrativa, cuyas resoluciones son a su vez controvertibles mediante el juicio de amparo ante el Poder Judicial de la Federación. Este proceso en la práctica puede tardar años, lo cual resta efectividad a este mecanismo.

En la práctica, los PPD han sido poco efectivos para remediar y disuadir prácticas violatorias del derecho a la protección de datos personales. Por ejemplo, según datos obtenidos de la Plataforma Nacional de Transparencia (INAI 2018), en el año 2018, el INAI únicamente recibió 251 solicitudes de PPD, de las cuáles únicamente en 6 se determinó revocar la respuesta del particular, solamente en 16 modificarla. Es decir, además de que el volumen de solicitudes es sumamente bajo, solamente en el 8.7 % de los PPD se concluyó y remedió una infracción al derecho de protección de datos personales. Lo anterior sin considerar los largos procesos de litigio ante el Tribunal Federal de Justicia Administrativa y ante el Poder Judicial Federal que podrían implicar que un número todavía más bajo de resoluciones puedan considerarse definitivas. Las anteriores cifras contrastan de manera importante con la actividad de otras autoridades de protección de datos en el mundo. Por ejemplo, la Autoridad Española de Protección de Datos (AEPD), que opera en un país con alrededor de un tercio de la población que tiene México, recibió 13005 reclamaciones (más de 50 veces la cantidad recibida por el INAI)

y emitió resoluciones 11839 veces, declarando una infracción en 604 ocasiones (27 veces más que el INAI).

Por otro lado, el INAI también posee otros dos mecanismos de supervisión y garantía del derecho de protección de datos personales: el procedimiento de verificación y el procedimiento de imposición de sanciones. El procedimiento de verificación permite al INAI abrir una investigación, de oficio o mediante denuncia, para determinar si una empresa ha incumplido la LFPDPPP. Por su parte, el procedimiento de imposición de sanciones permite al INAI sancionar a empresas respecto de las cuales se haya determinado que han violado la LFPDPPP, ya sea producto de un PPD o de un procedimiento de verificación.

De nuevo, estos procedimientos no han resultado en la imposición de sanciones significativas que permitan considerar un efecto disuasorio relevante. En el año 2018 el INAI únicamente impuso, en total, sanciones por poco más de 98 millones de pesos mexicanos (aproximadamente 5 millones de dólares estadounidenses).

Por lo tanto, si bien México cuenta con un diseño institucional robusto, con legislación y autoridades de protección de datos, en la práctica existen serios obstáculos para la realización efectiva del derecho de protección de datos personales. En particular, respecto de las EMNBD, existen limitaciones interpretativas para que les sean aplicables los mecanismos de protección de datos personales y, en cualquier caso, existen importantes obstáculos para que eventuales decisiones de la autoridad de protección de datos puedan obtener firmeza y ser implementadas con celeridad.

En aras de ejemplificar e ilustrar al lector sobre lo que se menciona en los párrafos que anteceden, es conveniente referirse al índice de responsabilidad corporativa de Ranking Digital Rights (2019), una herramienta de establecimiento de estándares destinada a alentar a las empresas de servicios en línea como de telecomunicaciones a cumplir con los estándares universales de derechos humanos que garantizan la libertad de expresión, privacidad y el manejo de datos personales.

En el informe publicado en mayo de 2019 fue evaluada la empresa América Móvil, de la que Telcel forma parte, por ser una de las más grandes empresas de telecomunicaciones del mundo y la más grande de la región. De acuerdo con la evaluación, pese a tener avances en su compromiso con el respeto a la libertad de expresión y derecho a la privacidad de sus usuarios, además de dar a conocer un nuevo entrenamiento para

trabajadores y programas sobre alertadores y derechos humanos, todavía no alcanza los marcadores básicos sobre transparencia.

Por ejemplo, la empresa no publica información sobre cómo maneja peticiones gubernamentales y privadas para bloquear contenido o dar información sobre usuarios. Asimismo, omitió proporcionar información suficiente sobre sus políticas que afectan la privacidad y la seguridad, de igual manera no aclara si notifica o no a sus usuarios cuando su información personal es solicitada por las autoridades (a pesar de tener una obligación legal de hacerlo).

Finalmente, Telcel no proporcionó información relacionada a posibles filtraciones masivas de datos. Si bien las empresas en México solo tienen la obligación de notificar a los usuarios cuando esta "afecta significativamente" sus derechos, Telcel no divulga esta información a sus usuarios. América Móvil tuvo una calificación de 25 de 100 posibles, lejos de la mejor empresa del rubro, Telefónica (España), con 57.

Recomendaciones

El régimen de protección de datos personales en México es inadecuado e insuficiente para garantizar la rendición de cuentas de las EMNBD. Por ello, resulta indispensable adecuar el marco normativo e institucional para garantizar que la creciente sofisticación de las prácticas de explotación de datos personales por parte de este tipo de empresas, no deje en indefensión a las personas y a la sociedad en general frente a sus múltiples impactos.

Algunas de las recomendaciones para corregir las insuficiencias del régimen de protección de datos personales en México son las siguientes:

1. Expandir normativamente y/o interpretativamente el alcance del *derecho de acceso*, de manera que las personas titulares de datos personales, la academia, los organismos garantes y la sociedad en general estén en posibilidad de conocer, identificar, estudiar y deliberar los impactos que la explotación de datos personales llevada cabo por las EMNBD tiene en los derechos humanos. En particular:
    b. El *derecho de acceso* establecido en la LFPDPPP debe modificarse o reinterpretarse de manera que el derecho a conocer "las generalidades del tratamiento" no impida a los distintos actores relevantes poder conocer con mayor detalle las

fuentes, finalidades, tratamientos y transferencias realizadas a partir de la explotación de datos personales.

c. El organismo garante de la protección de datos personales debe adoptar una interpretación amplia del concepto y debe utilizar sus facultades de verificación de manera más eficiente para generar más conocimiento respecto de la forma de operar de las EMNBD.

d. Debe promoverse mayor investigación académica sobre el alcance y repercusiones de la operación de la EMNBD en los derechos humanos dentro de México.

2. Deben promoverse un mayor desarrollo normativo e interpretativo de conceptos cruciales para garantizar la protección de datos personales y el respeto a otros derechos humanos a partir de las prácticas de las EMNBD. En particular:

a. Deben clarificarse los conceptos de "dato personal" y "dato personal sensible", de manera que dentro de ellos se encuentren comprendidos, al menos en algunas circunstancias, los datos biométricos, los identificadores en línea u otros identificadores únicos de dispositivos.

b. Debe otorgarse protección respecto de la inferencia de categorías sensibles a partir de la agregación de datos no sensibles.

c. Desarrollar limitaciones y protecciones específicas respecto del uso de técnicas de monitoreo en línea como el uso de *cookies,* etiquetas de pixel, entre otras.

d. Desarrollar limitaciones y protecciones específicas respecto de prácticas como la elaboración de perfiles, de manera que se garantice la transparencia, la autodeterminación informativa y se evite la discriminación.

e. Desarrollar limitaciones y protecciones específicas respecto de la toma de decisiones automatizadas y sus consecuencias. Al menos, debe garantizarse que la persona tenga derecho a conocer cuándo una decisión automatizada le afecte, así como conocer particularidades respecto del proceso y el resultado de la decisión.

f. Deben eliminarse las ambigüedades respecto de las obligaciones de notificación en casos de vulneraciones de seguridad. En concreto, debe establecerse la obligación de notificar cualquier vulneración ante el INAI y no limitar la

obligación de notificación al titular de datos personales solo respecto de las vulneraciones que "afecten significativamente los derechos patrimoniales o morales", como hoy indica el Artículo 20 de la LFPDPPP.

3. Dada la asimetría de poder y los límites intrínsecos a la capacidad de las personas de otorgar un consentimiento verdaderamente informado y libre, es indispensable establecer límites al consentimiento de tratamientos de datos personales que representen una afectación al interés público.
4. Modificar las normas reglamentarias de la LFPDPPP y la interpretación del INAI respecto del ámbito territorial de la ley, de manera que las EMNBD que, a pesar de tener su ubicación principal fuera del país, ofrecen servicios que impactan el ejercicio del derecho a la protección de datos personales de personas usuarias ubicadas en México, deban cumplir con lo que la LFPDPPP establece.
5. Robustecer las capacidades institucionales para la protección del derecho a la protección de datos personales. Algunas medidas que deben considerarse incluyen:
    a. Fortalecer las capacidades del INAI como regulador en materia de protección de datos personales, garantizándole recursos materiales y humanos suficientes para desempeñar su labor.
    b. Eliminar la posibilidad de impugnar las decisiones del INAI ante el Tribunal Federal de Justicia Administrativa y ofrecer únicamente el juicio de amparo como medio de control judicial de las decisiones del regulador.
    c. Eliminar obstáculos para el ejercicio de la facultad de verificación y aumentar los montos de sanción que el INAI puede imponer, de manera que los procesos de verificación, protección e imposición de sanciones sean verdaderamente disuasorias de conductas violatorias del derecho a la protección de datos personales.
    d. Facultar al INAI para ordenar mecanismos efectivos de indemnización de las personas titulares del derecho de protección de datos personales afectadas por conductas violatorias de la LFPDPPP.

e. Incentivar que las universidades desarrollen capacidades y promuevan la educación especializada en la protección de datos personales en México.
f. Fomentar la cooperación entre las autoridades de protección de datos personales y otras autoridades a nivel nacional e internacional.

6. Las EMNBD deben implementar medidas de autorregulación suficientes para prevenir, evitar, mitigar o remediar impactos en el derecho a la protección de datos personales, incluyendo la minimización de los tratamientos de datos personales, medidas efectivas de anonimización resilientes a técnicas de reidentificación y medidas de transparencia efectiva, entre otras.

Referencias

Agencia Española de protección de datos (AEPD). *Memoria 2018*. España: AEPD, 2019. Consultado julio 23, 2019. https://www.aepd.es/media/memorias/memoria-AEPD-2018.pdf

App Annie (2017). *Top App Matrix*. Consultado julio 23, 2019. https://www.appannie.com/en/

BBC Mundo. "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día". *BBC*, marzo 21, 2018. Consultado julio 23, 2019. https://www.bbc.com/mundo/noticias-43472797

Cabrera, Rafael. "Esta empresa que ayudó a la campaña de Trump ahora busca personal para las elecciones en México". *BuzzFeed News* octubre 31, 2017. Consultado julio 23, 2019. https://www.buzzfeed.com/mx/rafaelcabrera/esta-empresa-que-ayudo-a-la-campana-de-trump-ahora-busca#.idgaM5x7X

California Consumer Privacy Act (CCPA). 2018. Consultado octube 23, 2019. https://oag.ca.gov/privacy/ccpa

Chayka, Kyle. "Face recognition software: Is this the end of anonymity for all of us?" *The Independent*, abril 23, 2014. Consultado agosto 4, 2019. https://www.independent.co.uk/life-style/gadgets-and-tech/features/face-recognition-software-is-this-the-end-of-anonymity-for-all-of-us-9278697.html

CNNExpansión. "Amazon llega por primera vez a América Latina abriendo una tienda digital en México". *CNN Español*, 2015. Consultado

octubre 03, 2019. https://cnnespanol.cnn.com/2015/07/01/amazon-llega-por-primera-vez-a-america-latina-abriendo-una-tienda-digital-en-mexico/

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. 1 de junio de 2009.

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. México D.F.: Diario Oficial Mexicano. 21 de abril de 2009.

El Informador. "Vacío legal impide aplicar el derecho al olvido en México". *El Informador*, febrero 5, 2017. Consultado agosto 19, 2019. https://www.informador.mx/Tecnologia/Vacio-legal-impide-aplicar-el-derecho-al-olvido-en-Mexico-20170205-0093.html

Entrepreneur (2019). "Estas son las 10 startups mexicanas más populares en LinkedIn". *Entrepreneur*, septiembre 04, 2019. Consultado octubre 03, 2019. https://www.entrepreneur.com/article/339056

Grupo de Trabajo del Artículo 29. Opinión 03/2013 sobre la limitación de finalidad. Adoptada el 2 de abril de 2013, 00569/13/EN WP 203, 45. Consultado diciembre 20, 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-ecommendation/files/2013/wp203_en.pdf

Kúnfer, Sabine. "Clip–La evolución de la Startup más exitoa de México". *Medium*, mayo 14, 2018. Consultado octubre 3, 2019. https://medium.com/newco-shift-mx/clip-la-evoluci%C3%B3n-de-la-startup-m%C3%A1s-exitosa-de-m%C3%A9xico-d520bdc6ef51

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México D.F.: Diario Oficial de la Federación, 5 de julio de 2010.

Lineamientos del Aviso de Privacidad. México D.F.: Diario Oficial de la Federación. 17 de enero de 2013. http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

Martínez Laura. (2018). "Surgen más detalles sobre Cambridge Analytica y su conexión con México". *CNet*, marzo 30, 2018. Consultado julio 28, 2019. https://www.cnet.com/es/noticias/cambridge-analytica-conexion-con-mexico-channel-4/

Milenio (2019). "Amazon abre en México su centro de distribución más grande de Latinoamérica". *Milenio*, julio 31, 2019. Consultado octubre

3, 2019. https://www.milenio.com/negocios/amazon-abre-mexico-centro-distribucion-grande

Murata, Gloria, Neldy San Martín, José Raúl Linares. "Los 'gurús de datos de Trump' están en México y nadie sabe qué diablos hacen". *El Financiero*, enero 23, 2018. Consultado julio 25, 2019. https://www.elfinanciero.com.mx/nacional/los-gurus-de-datos-de-trump-estan-en-mexico-y-nadie-sabe-que-diablos-hacen

Newman Pont, Vivian y María Paula Ángel Arango. *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital*. Bogotá: Dejusticia, 2019. Consultado mes día año. https://www.dejusticia.org/publication/rendicion-de-cuentas-de-google-y-otros-negocios-en-colombia-la-proteccion-de-datos-digitales-en-la-era-digital/

Plataforma Nacional de Transparencia (INAI). "Información estadística. Procedimiento de Protección de Derechos correspondiente al primer trimestre de 2018". Consultado agosto 10, 2019. https://consultapublicamx.inai.org.mx/vut-web/faces/view/consultaPublica.xhtml#obligaciones

R3D. Red en Defensa de los Derechos Digitales. *Transparencia y Vigilancia en México, Lo que no sabemos sobre lo que el gobierno sabe de nosotros*. México: R3D. Red en Defensa de los Derechos Digitales, 2018. Consultado julio 23, 2019. https://r3d.mx/wp-content/uploads/r3d-transparenciayvigilancia.pdf

Red en Defensa de los Derechos Digitales (R3D), SocialTIC. *Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México*. México: R3D, ScoailTIC, mayo 2017. Consultado octubre 23, 2019. https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf

Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ce (Reglamento general de protección de datos). Abril 27 de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Reglamento de la Ley Federal de Protección de datos personales en posesión de los particulares. México D.F., Diario Oficial, 21 de diciembre de 2011

Ranking Digital Rights. *2019 RDR Corporate Accountability Index*. Ranking Rights, 2019. Consultado octubre 23 2019. https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019report.pdf

Telcel. "Aviso de publicidad", *Telcel* 2019. Consultado octubre 23, 2019. https://www.telcel.com/aviso-de-privacidad

Tufekci, Zeynep. "Facebook's Surveillance Machine". *The New York Times*, marzo 19, 2018. Consultado agosto 4, 2019. https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html?referer=https://t.co/wZEheBtu4U%3famp=1

UNHR United Nations High Commissioner for Human Rights. *The right to privacy in the digital age*, A/HRC/27/37 junio 30, 2014. Consultado agosto 4, 2019. https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

EMNBD Y PROTECCIÓN DE DATOS PERSONALES EN BRASIL, CHILE, COLOMBIA Y MÉXICO: LA EXPERIENCIA COMÚN

*Daniel Ospina-Celis**
*Juan Carlos Upegui Mejía***

Introducción

En este capítulo se ofrece una visión analítica y comparada de la forma en que algunas EMNBD capturan y tratan datos personales en Brasil, Chile, Colombia y México. Este ejercicio es posible a partir de los informes por país que integran este texto, los cuales, según la metodología descrita en la introducción de cada apartado, fueron elaborados a partir del análisis de las políticas de privacidad de los productos de diferentes empresas y de su relación con los gigantes de internet (GAFAM). Como capítulo de comparación, tiene la pretensión de dar cuenta —a partir de resaltar los hallazgos comunes— de los desafíos que los avances de la era digital les plantan a los derechos a la protección de la vida privada y de datos personales en la región.

Este informe comparativo es, a la vez, una reflexión sobre las dinámicas actuales de la economía digital y su impacto en los derechos

* Abogado de la Universidad de los Andes. Investigador de la línea de Tecnología, Transparencia y Derechos Humanos de Dejusticia.

** Profesor titular de la Universidad Externado de Colombia, doctor en Derecho de la Universidad Nacional Autónoma de México (UNAM). Director de la línea de Tecnología, Transparencia y Derechos Humanos de Dejusticia.

fundamentales, un somero ejercicio de derecho comparado —en punto a las legislaciones locales en materia de protección de datos personales—, y un modesto aporte a la literatura sobre la relación entre empresas y derechos humanos[1] en los entornos digitales.

El derecho a la protección de datos personales es un derecho humano derivado del derecho a la protección de la vida privada. En el contexto universal, el derecho a la protección de la vida privada fue reconocido en el Artículo 12 de la Declaración Universal de Derechos Humanos (Asamblea General de las Naciones Unidas 1948) y en el Artículo 17 del Pacto de Derechos Civiles y Políticos (Naciones Unidas 1966). El Comité de Derechos Humanos, interpretando estas disposiciones, ha indicado que "toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos" (1988) y de saber cuáles son esos datos y cómo son utilizados. Recientemente, la Asamblea General de las Naciones Unidas adoptó la Resolución A/C.3/71/L.39 (2016), sobre derecho a la privacidad en la era digital, en la que exhorta a Estados y empresas a cumplir su obligación de respetar los derechos humanos, especialmente el derecho a la privacidad en la era digital.

En el contexto europeo, el derecho a la protección de datos personales fue objeto del Convenio 108 de 1981, del Consejo de Europa, el primer instrumento internacional que tuvo como finalidad garantizar a cualquier persona física "su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal". Asimismo, ha sido reconocido, como derecho fundamental autónomo, en el Artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, adoptada en el año 2000 — y vinculante desde el 2009— como el derecho de toda persona "a la protección de los datos de carácter personal que le conciernan" (Unión Europea 2000). Por su parte, en el contexto del derecho de la comunidad europea se adoptó, en el año 1995, la Directiva 95/46/CE del Parlamento europeo y del Consejo que reguló con amplitud "la protección de las personas físicas en lo que respecta al tratamiento de datos personales". Esta Directiva fue recientemente derogada por el

1 En desarrollo de esta idea, el Consejo de Derechos Humanos de las Naciones Unidas adoptó los Principios Rectores sobre las Empresas y Derechos Humanos (Asamblea General de las Naciones Unidas 2011). Los Principios Rectores sobre las Empresas y los Derechos Humanos se encuentran recogidos en el documento HR/PUB/11/04 (Naciones Unidas 2011).

nuevo Reglamento General de Protección de Datos, Reglamento (UE) 2016/679, cuyo revelado propósito ha sido la actualización del régimen de protección de datos personales para ponerlo a tono con las nuevas prácticas de la economía digital.

En el ámbito latinoamericano no existe todavía un instrumento internacional vinculante que reconozca y que regule el derecho a la protección de datos personales. Sin embargo, sí ha sido reconocido en instrumentos de *soft law*, como la declaración de Santa Cruz de la Sierra, adoptada en 2003, al final de una cumbre iberoamericana de Jefes de Estado, que, en su numeral 45, reconoce la protección de datos personales como un "derecho fundamental de las personas". Adicionalmente, la Red Iberoamericana de Protección de Datos (2017) aprobó en 2017 los *Estándares de protección de datos personales para los Estados iberoamericanos* en donde se reconoce a la protección de datos personales como un derecho humano fundamental (considerando 1) de especial importancia en la era digital.

De forma paralela a los desarrollos sobre el derecho a la protección de la vida privada en el ámbito universal y regional, los ordenamientos jurídicos de los países objeto de análisis han reconocido constitucional y legalmente el derecho a la protección de datos. En Brasil, el derecho al *habeas data* se encuentra reconocido en el numeral 71 del Artículo 5º de la Constitución de 1988. En específico, se garantiza un mecanismo procesal para conocer la información propia que conste en bases de datos públicas y para la rectificación de datos. Casi 30 años después de expedida la Constitución, se promulgó en Brasil la Ley Nº 13.709 de 2018, que regula integralmente la protección de datos personales.

De manera similar al caso brasileño, el Artículo 15 de la Constitución Política de Colombia de 1991 reconoce el derecho de toda persona a conocer, actualizar y rectificar la información personal que se encuentre recogida en bancos de datos públicos o privados. En desarrollo de esta disposición, el Congreso colombiano expidió, después de 20 años de la reforma constitucional, la Ley 1581 de 2012, una normativa general sobre el derecho a la protección de datos personales.

En Chile, el derecho a la protección de datos personales fue incluido en la reciente reforma constitucional de 2018, que lo incorporó a la disposición del numeral 4º del Artículo 19. Según la cual, se asegura a todas las personas "la protección de sus datos personales. El tratamiento y la protección de estos datos se efectuará en la forma y condiciones

que determine la Ley". No obstante, hace más de 20 años, en 1999, el Congreso chileno había expedido la Ley 19.628, una de las primeras en regular la protección de datos personales en la región. Ante la antigüedad de la normativa chilena, la nueva reforma constitucional y los avances tecnológicos desde 1999, el Congreso chileno se encuentra discutiendo una actualización de su normativa de protección de datos.

Por otro lado, desde el año 2009, el Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce explícitamente el derecho a la protección de datos personales, al acceso, rectificación y su cancelación, y a manifestar su oposición al tratamiento de información personal. De las cuatro disposiciones constitucionales invocadas, esta es la más completa y comprehensiva. A partir de esta reforma constitucional, en 2010 se promulgó la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Teniendo en cuenta que la protección de datos personales es un derecho humano reconocido internacionalmente y un derecho constitucional fundamental en los Estados comprendidos en este estudio, el presente capítulo busca: primero, identificar algunos elementos característicos o relevantes de las prácticas de acopio y tratamiento de datos de las EMNBD estudiadas en Brasil, Chile, Colombia y México; segundo, identificar la manera en que las legislaciones locales en los países referidos regulan (o no) dichas prácticas, y si tal regulación es adecuada y suficiente; y tercero, esbozar algunas recomendaciones que sirvan de insumo para una futura regulación regional, que fortalezca la protección de los derechos asociados con el tratamiento de datos personales y permita una verdadera rendición de cuentas de las EMNBD que capturan y tratan los datos personales de las y los ciudadanos en la región.

Para estos efectos, primero, se analizará qué aspectos comunes existen en la forma de operar de las EMNBD, lo que supone, además, identificar los riesgos que enfrentan los cuatro países en cuanto al uso y análisis de datos en la era digital. Enseguida, se analizarán las carencias regulatorias de las legislaciones en cuestión, de cara al tratamiento de datos personales en la era digital y sus desarrollos tecnológicos. Por último, se analizará la figura de la autoridad de protección de datos y sus capacidades de hacer rendir cuentas a las EMNBD que no cumplan con la legislación.

1. Aspectos y riesgos comunes en la forma de operar de las EMNBD

Los estudios por país sobre las prácticas de las EMNBD revelan cierta convergencia en las formas de recolección de datos, y en las motivaciones y técnicas de análisis con las que se adelanta el tratamiento de datos personales en el contexto de la economía digital. Esto es así, a pesar de que, como es obvio, cada empresa adelanta el tratamiento de datos personales de sus usuarios/clientes a partir de su estrategia de negocio. A continuación, se presentarán los aspectos comunes a la mayoría de las EMNBD analizadas —más de cuarenta compañías— que operan en Brasil, Chile, Colombia y México y sus implicaciones para el derecho a la protección de datos de los usuarios de servicios digitales. Para esto, se tendrán en cuenta las categorías que fueron definidas en la metodología de la investigación: 1) fuentes de datos, 2) tratamiento y 3) finalidades del tratamiento.

1.1. Fuentes de datos

La mayoría de las EMNBD analizadas reconoce que recolecta datos de sus usuarios/clientes mediante tres fuentes: 1) los datos proporcionados directamente por el usuario/cliente, 2) los datos recolectados por medio del *web tracking* o monitoreo, y 3) los datos proporcionados por terceros o socios estratégicos. Estas tres fuentes son tan comunes para la economía digital que, en México, por ejemplo, Amazon y Snapchat reconocen abiertamente en sus políticas de privacidad que utilizan estas tres categorías como 'fuentes' de datos.

1.1.1. Recolección directa en la fuente: el registro del titular de los datos

Los datos proporcionados por el usuario/cliente son usualmente recolectados en la etapa de registro en la plataforma y, por tanto, son los datos sobre los que el titular tiene mayores posibilidades de conocimiento y control, y de incidir en su recolección. Es común en las EMNBD estudiadas requerir la creación de una cuenta o perfil para el uso del producto/servicio ofrecido. Esto sucede con iFood y Magazine Luiza en Brasil; AIRA, Facebook y PedidosYa en Chile; Facebook, Instagram y Uber, entre otras, en Colombia, y Amazon, Snapchat y PayClip en México. En todos estos casos, las aplicaciones o los servicios no pueden ser utilizados

sin la creación de un perfil. Los datos que usualmente se recolectan por esta vía son: nombre, correo electrónico, edad, número de teléfono del titular, dirección postal, y datos de medios de pago —número de tarjeta de crédito, franquicia, etc. —, en los casos de las EMNBD dedicadas a la venta y entrega de bienes y servicios.

Poca claridad sobre el tipo de datos recolectados

Una circunstancia común en las políticas de privacidad de las EMNBD analizadas en los cuatro países es que en muy pocas se indica de forma exhaustiva cuáles son los datos recolectados. En México, la política de privacidad de Payclip indica que se recolecta un listado de datos de manera enunciativa mas no limitativa; por su parte, la política de privacidad de Amazon utiliza términos vagos y ambiguos, e incurre en la práctica —prohibida por los lineamientos del aviso de privacidad mexicanos[2]— de utilizar ejemplos de los datos recabados, sin agotar de forma exhaustiva el listado de los datos objeto de recolecta. Esta práctica revela, sobre todo, la falta de transparencia sobre la totalidad de datos personales que efectivamente son recogidos, y la imposibilidad del titular de los datos, primero, de conocer cuáles de sus datos personales serán objeto de tratamiento y segundo, de adelantar cualquier tipo de control sobre los tratamientos posteriores.

Uno de los casos más preocupantes sobre este aspecto lo ofrece Brasil. Al estudiar el caso del servicio de *streaming* de Amazon Prime Video, que se comercializa por medio de la suscripción de un contrato con Vivo, empresa de telecomunicaciones filial de Telefónica, el estudio reveló la concurrencia de dos políticas de privacidad (la de Vivo y la de Amazon Prime Video) con el agravante de que, en el caso de esta última, las políticas solo están disponibles en idioma inglés. Al usuario le son aplicables las dos políticas de privacidad, sin que sea muy claro qué sucede en caso de contradicción entre estas. En este caso, no solo no hay claridad sobre la extensión del universo de los datos personales objeto de recolección, sino que un consumidor promedio tiene dificultades para

2 Los lineamientos del aviso de privacidad son un acto administrativo, expedido por la autoridad nacional de protección de datos mexicana (en este caso el INAI) donde se fijan reglas para establecer la política de privacidad de los sujetos obligados por la Ley de Protección de Datos Personales en Posesión de Particulares. (Estados Unidos Mexicanos 2013).

encontrar la política de privacidad aplicable, y solamente un consumidor cualificado —con el tiempo suficiente y conocimientos de la lengua inglesa— podría tener una idea más o menos cercana sobre el tipo y la extensión de los datos objeto de recolección.

Los datos sensibles

Algunas EMNBD solicitan información que, según las legislaciones de cada país, corresponden a datos sensibles[3]. Los datos sensibles, en general, tienen una protección adicional, al ser considerados una categoría especial de datos personales, pues atañen a la esfera más íntima de las personas y su tratamiento inadecuado podría generar discriminación. Estos corresponden usualmente a información relacionada con las creencias religiosas, ideología política, características físicas o morales, hábitos (en el caso chileno), datos biométricos y de salud, entre otros. El caso de los 'hábitos' es destacable. El perfilamiento y la fidelización de los usuarios/clientes son actividades centrales para las EMNBD. Ninguno de estos importantes activos de la economía digital puede obtenerse o comercializarse si no hay tratamiento de datos personales que constituyen los 'hábitos' de consumo o de conducta de los clientes/usuarios. La cuestión es tan delicada que, en el contexto de la discusión del nuevo régimen de protección de datos chileno, se ha propuesto la eliminación de los 'hábitos' como categoría de datos sensibles. Una situación considerada por los expertos consultados en el caso chileno como un claro retroceso frente al régimen jurídico vigente. El punto es crítico, pues existe un claro interés de las EMNBD en que este tipo de información no sea calificada como información sensible. En Colombia, Tinder y Unilever solicitan en su etapa de registro, de manera obligatoria, la entrega de información sensible y así lo hacen explícito. De otra parte, la política de privacidad de EasyTaxi también en Colombia indica explícitamente que "[n]inguno de los datos que serán objeto de tratamiento tienen el carácter de dato

---

3 En Chile, los datos sensibles se encuentran regulados en la Ley N° 19.628, Artículo 2, literal g; en Colombia su regulación está en la Ley 1581 de 2012, Artículo 5. México regula los datos sensibles por medio de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Artículo 3, numeral VI y Artículo 9. Finalmente, en Brasil el tratamiento de datos personales sensibles se encuentra regulado en el numeral II del artículo 5 y en los artículos 11, 12 y 13 de la Ley N° 13.709 de 14 de agosto de 2018.

sensible". Esta situación podría considerarse una buena práctica, en tanto la empresa se abstiene voluntariamente de recolectar datos sensibles, bajo el entendido que no son necesarios para la prestación del servicio.

Los datos 'necesarios'

Las legislaciones de protección de datos de Brasil, Chile, Colombia y México no regulan directa y explícitamente la entrega voluntaria de datos personales en el escenario digital. Estas conductas son reguladas por las normas generales sobre el consentimiento para el uso y recolección de datos y por el principio de proporcionalidad-necesidad. Las EMNBD deben informar adecuadamente qué datos están recolectando y garantizar la voluntariedad con la que el usuario los entrega, especialmente si se trata de datos personales sensibles. Los casos de las políticas de uso de Facebook y de Falabella en Chile son relevantes en este punto, porque obligan al usuario a entregar información sobre su sexo/género como requisito para usar el servicio. ¿Es realmente *necesario* entregar este dato a Facebook o a Falabella para hacer uso de la red social o de los servicios online de esta *retailer,* o se trata de un requisito desproporcionado por parte de la EMNBD que muchos —tal vez con tal de poder hacer uso de Facebook o de Falabella *online*— están dispuestos a soportar? Algunos procesos de registro no discriminan entre los distintos tipos de información personal (sensible/no sensible), no permiten espacios de libertad del usuario para negarse a entregar los datos sensibles y, en todos los casos, el argumento que justifica su recolección "la personalización de las comunicaciones" (los mensajes, según su política, cambian dependiendo si se trata de hombres o mujeres) no parece suficiente. Esta situación es ilustrativa del desbalance existente entre empresa y usuario, incluso en un escenario de aparente consentimiento libre.

Datos relacionados con pagos

Otro tipo de datos usualmente recolectados, proporcionados por el usuario/cliente directamente, se relacionan con la información indispensable para realizar pagos y otros negocios jurídicos mediante la plataforma. Datos como el nombre del banco, el número de cuenta y/o el número de tarjeta de crédito del usuario, la franquicia, fecha de vigencia, etc., son recolectados por las EMNBD que facilitan la celebración de contratos de compraventa mediante sus plataformas. Asimismo, información relacionada con los productos seleccionados, histórico de compras, dirección

de correspondencia o envío y monto de la transacción son susceptibles de ser recolectados. Es preocupante que empresas que se dedican a la venta o intermediación y que, debido a la naturaleza del servicio prestado, recolectan información sobre las compras y transacciones, no sean completamente transparentes al respecto. Falabella y PedidosYa, dos plataformas que ofrecen servicios de comercialización de bienes y servicios en Chile, no ponen de presente en sus políticas de privacidad que recolectan este tipo de información. Lo anterior, en contraste con los términos de servicio de Ifood (Brasil) o de Facebook, en los que se especifica que se hace tratamiento de "información de pago, como el número de tu tarjeta de crédito o débito"[4].

1.1.2. Recolección de datos mediante web tracking

Frente a los datos recolectados por medio de *web tracking* o monitoreo, esto es, información sobre los sistemas y herramientas de internet utilizados por un usuario al navegar o utilizar una plataforma, la situación supone una valoración especialmente técnica. Esta faceta de recolección incluye, principalmente, la información sobre la actividad en la aplicación (denominada *online data*) que se refiere a datos como tiempo de uso de la aplicación, detalles de las compras, historial de búsquedas, mapa de calor del *mouse*, interacciones dentro de la plataforma, entre otros. También incluye información sobre los dispositivos o sistemas usados por el usuario (*log data*), como la aplicación en sí misma, la dirección IP (protocolo de internet) desde la que se conecta, el tipo de dispositivo, la red a la que está conectado, la versión del navegador, preferencias de idioma o zona horaria.

La característica central de esta fuente de datos es que la información se recolecta con cada uso de la aplicación o con cada acceso a la página web y, por tanto, puede indicar patrones y/o hábitos del usuario/cliente/consumidor de gran interés para las EMNBD. Gracias a los datos recolectados por medio del *web tracking*, en donde en principio parece no haber recolecta de datos personales, las compañías pueden perfilar a sus usuarios y ofrecer servicios personalizados. Facebook, en los casos chileno y colombiano, es la que describe con mayor detalle los métodos

4 Al respecto, ver el apartado "Información sobre transacciones realizadas en nuestros Productos" de las políticas de privacidad de Facebook en https://www.facebook.com/policy

de monitoreo que emplea. Categoriza los datos obtenidos en razón de los mecanismos utilizados, así: 1) atributos de dispositivos, 2) operaciones de dispositivos, 3) identificadores, 4) señales del dispositivo, 5) datos de configuración de dispositivos, 6) red y conexiones, 7) datos de *cookies*[5].

Web tracking y cookies

El *web tracking* se refiere a la práctica de recolectar información (incluyendo datos personales) generada al navegar por internet. La información, en principio y en apariencia, no es personal, pero sí que lo es en tanto puede ser vinculada a una persona identificable mediante un identificador de usuario. La información recolectada no necesariamente se produce al momento de interactuar con la página web, sino que puede corresponder a información propia del dispositivo en el que se realice la navegación. Es importante tener en cuenta que, para el sistema, es fundamental identificar al usuario-equipo porque eso permite facilitar la experiencia de navegación. Por ejemplo, esta identificación permite mostrar una página web en determinado idioma, el del usuario, que al navegar por una red social la sesión se mantenga activa o que los productos que se introducen en el carrito de compras no se borren al iniciar el proceso de pago en línea.

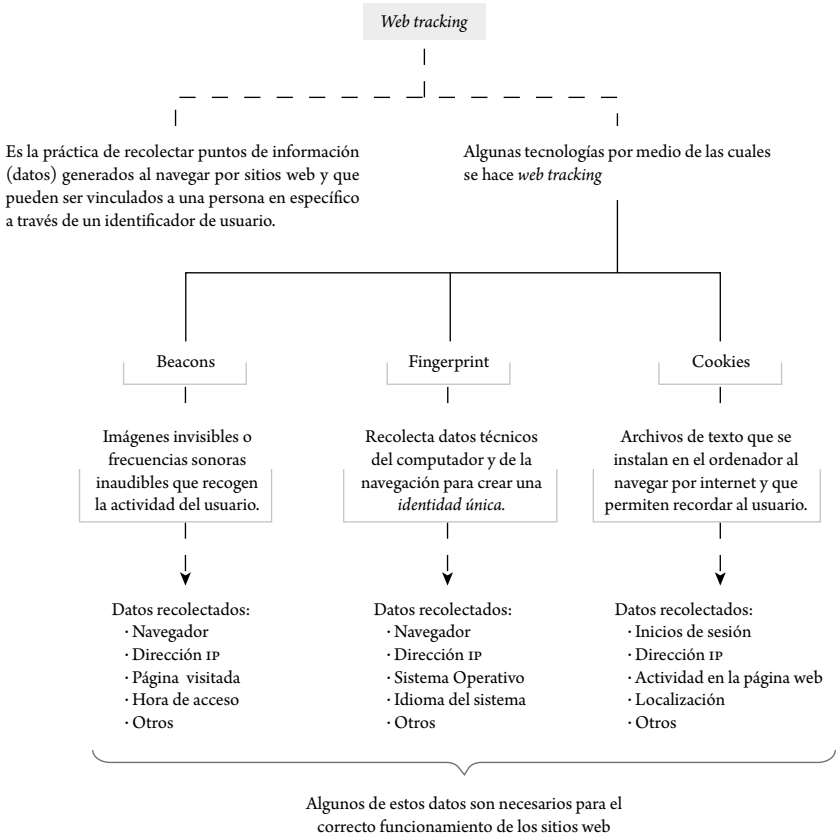
Para realizar *web tracking* se pueden usar diversas herramientas que, dependiendo de sus características técnicas, recolectarán cierto tipo de información. En términos generales, existen dos tipos de tecnología para realizar *web tracking*: el *stateful web tracking* (con estado) y el *stateless web tracking* (sin estado). El primero implica la instalación de un archivo en nuestros dispositivos, mientras que el segundo se basa en la recolección de información (usualmente datos técnicos del dispositivo), sin la necesidad de instalar archivo alguno. Las cookies son un ejemplo de tecnología *stateful*, mientras que *fingerprint* y *beacon* son muestras de tecnología de tipo *stateless*. En el gráfico 1 se muestra una explicación de *web tracking* y algunas de las tecnologías que lo posibilitan.

Teniendo claro qué es *web tracking* y las tecnologías que lo posibilitan, ahora procederemos a hacer una breve referencia a las *cookies* como herramientas específicas por medio de las cuales se hace el seguimiento web. A pesar de la relevancia de otras tecnologías usadas para realizar

5 Ver: https://www.facebook.com/about/privacy/update

web tracking, discutiremos únicamente las *cookies* debido a su particular relevancia en las políticas de privacidad de las EMNBD analizadas en este libro.

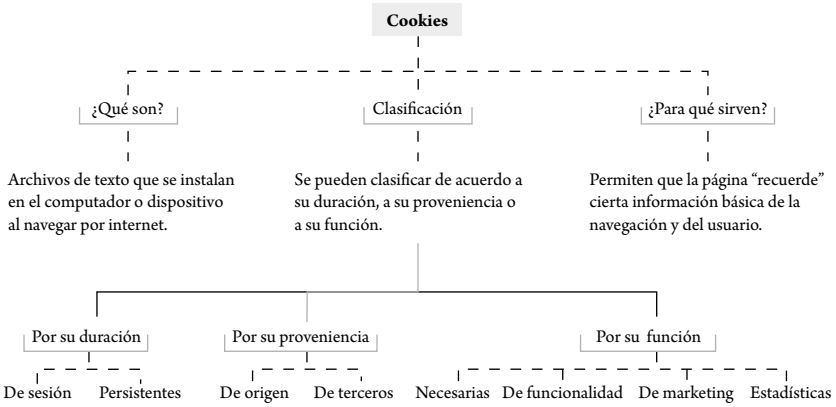
Gráfico 1. *Web Tracking*



Las *cookies* son pequeños archivos de texto que se instalan en los dispositivos al navegar por internet. Su función principal (de hecho, este fue su uso inicial) es facilitar la navegación del usuario en tanto se encargan de 'recordar' cierta información útil para los sitios web. Por ejemplo, permiten que el sitio reconozca que se ha iniciado sesión o que se ha seleccionado determinada opción/configuración. Hoy en día, sin embargo, las *cookies* se usan para mucho más que permitir la adecuada navegación por los sitios web. Uno de sus usos más comunes, de hecho, es la recolección de información personal con fines publicitarios o de marketing.

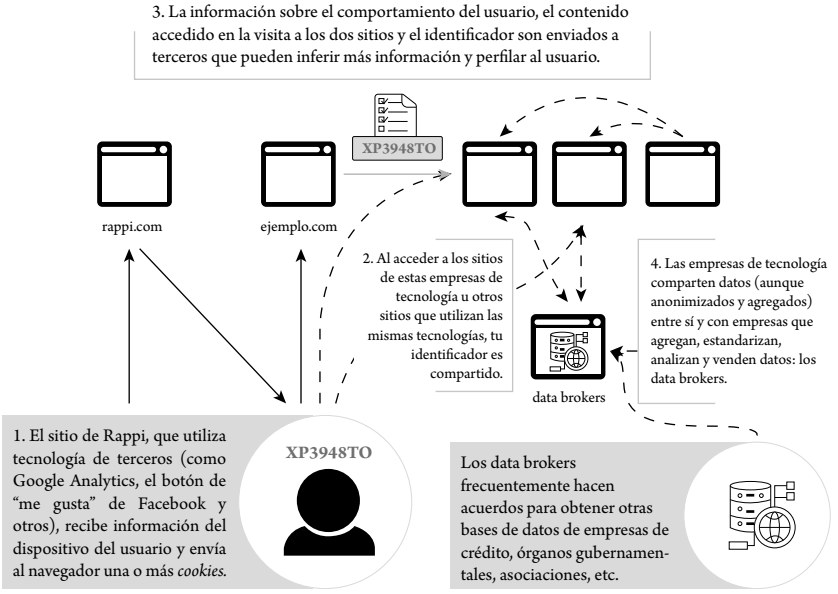
Principalmente, las *cookies* se pueden clasificar utilizando tres criterios:1) su duración, 2) su origen y 3) su función. En cuanto a su duración —es decir, cuánto tiempo van a permanecer en el dispositivo—, las *cookies* pueden ser de sesión (se borran al cerrar el navegador o la sesión) o persistentes (permanecen tras cerrar el navegador hasta que sean borradas o caduquen). Si tenemos en cuenta su origen, las *cookies* puede ser de origen (*first-party cookie*) o de terceros. Cuando son de origen, significa que las instala la página web que estamos visitando, mientras que, si son de terceros, quien las instala es otro actor diferente a la página en la que navegamos. Por último, en cuanto a su función, las *cookies* pueden ser necesarias (sin ellas no es posible la navegación, e.g. compras en línea), de funcionalidad (mejoran la experiencia de navegación, e.g. reconocer el idioma), estadísticas (agregan datos sobre cómo se usa la web) o de marketing (buscan adaptar la publicidad que recibe el usuario para que se ajuste a sus gustos). En el gráfico 2 se muestra una representación visual de qué son las *cookies* y su clasificación.

Gráfico 2. Representación del funcionamiento de las cookies



Lo anterior se enmarca en un contexto en el que, como queda claro de las prácticas de las EMNBD analizadas, las empresas comparten datos entre ellas y con empresas de datos o *data brokers*. En el gráfico 3, se muestra una representación gráfica del proceso de recolección de datos por medio de las páginas web y de la transferencia de datos entre empresas.

Gráfico 3. Representación gráfica del proceso de recolección y transferencia de datos



Estatus de los datos obtenidos mediante web tracking

El entendimiento sobre el carácter (personal o no) de los datos obtenidos a partir del *web tracking* es un asunto crítico en el contexto de las prácticas de recolección de datos. Por ejemplo, la brasileña iFood, una aplicación para la venta de comida a domicilio, estima que la información sobre las actividades de los usuarios en el sitio web o en la aplicación de la empresa tiene la característica de no ser personal, en tanto es agregada y supuestamente no permite la identificación de cada usuario. La política también clasifica "la edad del individuo, las preferencias individuales, el idioma, el CEP y el código de área" como 'datos no personales'[6]. Una situación similar sucede en el caso de Social Miner, *start-up* de marketing digital en Brasil, cuya política de privacidad niega la condición de información personal de los datos recolectados a partir del uso de *cookies* persistentes y de sesión cuando estos se utilizan para estudios generales de mercado. Social Miner define que "los datos usados para los estudios

6 iFood (2018). Política de Privacidade. Disponible en: https://www.iFood.com.br/privacidade

generales de comportamiento del consumidor se obtienen eliminando la información personal de los usuarios" caso en el cual no configuran un dato personal y sí un "mero conjunto de datos anónimos para fines de estudio e investigación". La definición de los datos recolectados por medio del *web tracking* como información no personal no es exclusiva de las empresas brasileñas. En Colombia, Duety y Apple también lo consideran así en tanto, argumentan, estos datos no están vinculados con el usuario/cliente, sino con una dirección IP.

Tratamiento y cookies

Es común que las empresas estudiadas en Brasil, Chile, Colombia y México indiquen en sus políticas de privacidad que usan *cookies* para recolectar información de sus usuarios. Las *cookies* son una fuente discreta de captura de datos personales. Su relevancia es tal que varias de las EMNBD han decidido hacer explícita la finalidad y el tipo de información que se recaba a partir de estas. Son tan importantes para las compañías analizadas, y para el *big data* en general, que varias de ellas tienen una política de *cookies* propia, separada de su política de privacidad. Este es el caso de Snapchat en México, PedidosYa en Chile y Social Miner en Brasil que, debido al rol preponderante de recolección de datos que realizan mediante *cookies*, crearon un documento destinado exclusivamente a explicar a sus usuarios cómo funcionan las *cookies* de sus productos. Asimismo, Facebook tiene un apartado dentro de su política de datos dedicada exclusivamente a *cookies* y otras tecnologías de almacenamiento en la que explica su uso en detalle.

Por ejemplo, Snapchat, en México, indica en su política de privacidad que utiliza las *cookies* para distintos fines (seguridad, personalización, desempeño) y las clasifica en 4 categorías: 1) necesarias (para detectar riesgos de seguridad y corregirlos); 2) preferencias (recordar ajustes, mejorar la experiencia del usuario); 3) desempeño (información sobre el uso del sitio web con la finalidad de monitorear y mejorar el desempeño) y 4) mercadotecnia (ofrecer publicidad, anuncios y campañas publicitarias especializadas y dirigidas a los usuarios según su perfil y sus intereses). Por su parte, la chilena PedidosYa, en su apartado de *cookies*, indica con detalle que emplea tres tipos: analíticas, de sesión y persistentes, e indica que estas recopilan "información acerca de su computadora, y acerca de sus visitas y uso de este sitio web incluyendo su dirección IP, ubicación

geográfica, tipo de navegador, fuente de referencia al sitio, duración de las visitas y número de vistas por página".

1.1.3. Los datos suministrados por terceros

Los datos proporcionados por socios estratégicos o por terceros son la tercera fuente de datos de las EMNDB analizadas. Teniendo en cuenta la forma en que funciona el comercio de datos personales y su importancia para la economía digital, podría suponerse que las empresas reconocen abiertamente que obtienen datos de terceros y que informan al usuario/cliente de esta situación. Sin embargo, esto no sucede en la práctica. De las cuatro EMNBD analizadas en Chile, solo Facebook reconoce en su política de privacidad que recolecta datos mediante socios estratégicos —los cuales, debido a su carácter de gran empresa de internet y a la posibilidad de vincular casi cualquier página o plataforma con botones sociales, son millares alrededor del mundo—. Esto supone que el resto de empresas estudiadas en ese país o no usan datos proporcionados por terceros o que al menos no son transparentes al respecto. Por otra parte, hay buenos ejemplos de transparencia en este punto, como el caso de la aplicación *8fit Workouts and Meal Planner*, en Colombia, que incluye los nombres de todas las aplicaciones de terceros que se conectan a la aplicación y los socios con los que comparte información.

La tercerización de la recolección de datos: un problema de transparencia

La recolección de datos por medio de socios o terceros, si bien no necesariamente implica un problema de legalidad en sentido estricto (aunque podría llegar a serlo), sí está acompañada por una falta generalizada de transparencia por parte de las EMNBD estudiadas. En Colombia, por ejemplo, Spotify indica en sus términos de servicio que utilizará datos personales cuando se le haya dado autorización a un tercero o cuando la empresa tenga un interés legítimo en ello. ¿Cuáles son los socios estratégicos de los que se nutren las EMNBD para recolectar datos? Este tipo de información no suele estar disponible en las políticas de privacidad. Otro ejemplo de esta situación lo ofrece Telcel en México. En sus políticas de privacidad reconoce que puede recolectar datos por medio de fuentes indirectas, como comunicaciones con otros o de terceros con los que Telcel tenga acuerdos comerciales, o incluso, que podrá recoger datos personales de fuentes de acceso público (como redes sociales).

No se indica, sin embargo, cuáles son esos socios comerciales de los que obtiene información, ni qué tipo de información recolecta, ni tampoco cómo adelanta el rastreo de internet para la recolecta de datos.

Por otro lado, la *start-up* brasileña Social Miner indica en sus políticas de privacidad que hace uso de datos de terceros como Google y Facebook mientras que, a su vez, les entrega datos a estas compañías. Este intercambio de información pone de presente una situación común a casi todas las EMNBD: su relación comercial (de ida y vuelta) con Google, Amazon, Facebook, Apple y/o Microsoft. En este caso en concreto, Social Miner ofrece la posibilidad de conectarse por medio de Facebook, lo cual le otorga a la *start-up* información sobre inicio de sesión en la plataforma y a la red social la información de navegación en Social Miner. Se trata, mejor dicho, de una alianza en la que ambas compañías sacan provecho de los datos, mientras que el usuario aumenta su comodidad y/o facilidad de conexión.

La matryoshka: los botones de inicio y las páginas propias en redes sociales

La relación entre las EMNBD y GAFAM tiene, al menos, dos aristas. Por un lado, varias empresas usan en sus aplicaciones móviles o en sus páginas web botones de inicio de sesión o herramientas de interoperabilidad que permiten el intercambio de datos. Por el otro, las EMNBD más pequeñas tienen páginas en redes sociales con el fin de hacer publicidad y atraer nuevos clientes, o utilizan los servicios de Google Analytics para efectos de medir el funcionamiento de sus aplicaciones y las interrelaciones con sus usuarios/clientes. En Chile, por ejemplo, AIRA, Falabella y PedidosYa tienen páginas en Facebook, mediante las cuales comparten publicidad y generan un vínculo más cercano con sus seguidores. Lo anterior permite que Facebook recolecte información adicional de los usuarios de las aplicaciones, mientras que le ofrece a estas su plataforma para difundir mejor y a más personas su contenido. En el caso brasileño, iFood afirma que podrá compartir datos con sus socios, con el fin de desarrollar campañas de marketing más asertivas, aunque dice que "solamente compartirá datos con aquellos socios que tengan una política de privacidad que ofrezca niveles compatibles de protección a lo ofrecido" por su política. Además, los terceros que realicen marketing dentro de la aplicación o el sitio web de iFood, o sea, que promuevan la publicidad de productos a terceros en esos espacios, "pueden utilizar *cookies* y otras tecnologías propias en

los servicios de iFood, tales como Facebook, Google Analytics y Double Click" para evaluar el funcionamiento de las campañas de marketing. Una situación similar ocurre con la brasileña Social Miner, caso en el cual siempre que un usuario navegue en el sitio web de la empresa, la visita es transformada en un dato procesado por Google Analytics.

El intercambio de datos entre empresas aparece caracterizado por la opacidad. Sobre todo, cuando el producto en cuestión es el resultado de una alianza entre dos empresas o cuando una misma empresa es dueña de dos productos distintos. El primer escenario es el que se da en el caso de Amazon Prime Video en Brasil, el cual es un producto de Amazon.com, Inc., pero que se ofrece por medio del operador de telefonía Vivo. Aunque un usuario en Brasil puede acceder a los términos de servicio de Amazon Prime Video, estos no se encuentran disponibles en portugués y, además, no establecen claramente si los datos recolectados por Vivo se consideran datos de terceros o cuál es la relación entre las dos empresas en este punto. El segundo escenario (dos productos, un dueño) se da en el caso de la empresa Facebook que es dueña, simultáneamente, de Facebook, Instagram y WhatsApp. Si bien las políticas de privacidad de esta última en Colombia indican que al momento de compartir información con terceros —incluso con aquellos que hacen parte del grupo empresarial de Facebook— WhatsApp exige que estos cumplan con sus condiciones, no es claro qué sucede en el caso contrario: cuando son terceros (hagan o no parte de Facebook) quienes comparten datos con WhatsApp.

La política de uso de datos de Facebook en cuanto a su relación con otras aplicaciones es un caso especial. Como muestra de la interoperabilidad entre Facebook y otros, esta informa que los socios "proporcionan información sobre las actividades que realizas fuera de la plataforma, incluidos los datos sobre el dispositivo que utilizas, los sitios web que visitas, las compras que realizas, los anuncios que ves" y demás[7]. En todo caso, esta no es la única referencia al 'compartimiento' de datos en las políticas de privacidad de Facebook. Esta vez, sin embargo, los datos fluyen en sentido contrario. Según la información proporcionada por esta red social, "cuando decides utilizar aplicaciones, sitios web u otros

7 Esta explicación se encuentra en la sección de "Información en poder de los socios" de las políticas de privacidad de Facebook en https://es-es.facebook.com/privacy/explanation

servicios de terceros que usan nuestros Productos o están integrados en ellos, estas plataformas pueden recibir información acerca de tus publicaciones o del contenido que compartes". Asimismo, "los sitios web y las aplicaciones que usas pueden tener acceso a tu lista de amigos de Facebook"[8].

1.2. El tratamiento

En términos definitorios, el tratamiento de datos personales incluye prácticamente cualquier actividad relevante relacionada con datos personales. Esto incluye, entre otras, las actividades de recogida, cesión, transferencia, transmisión de datos, independientemente de su modalidad, de las circunstancias de tiempo, modo y lugar y de quiénes intervengan en dichas actividades. Algo de esto ya lo presentamos en el acápite anterior al describir las prácticas de *web tracking*, el uso de *cookies* y otras formas más sutiles de compartir la información. En el presente apartado, nos concentraremos brevemente en las prácticas de tratamiento de datos de las EMNBD relacionadas con el análisis de la información.

El análisis y la clasificación de la información personal, como formas de tratamiento, son comunes a varias de la EMNBD. Estas formas de tratamiento tienen la finalidad de generar soluciones de información con valor agregado, al identificar, por ejemplo, patrones de consumo y preferencias de usuarios. Estos activos son muy útiles para mejorar la experiencia de los usuarios, fidelizar la clientela y optimizar las actividades y las estrategias de mercadeo y publicidad de productos y servicios de terceros.

Los resultados de los análisis y procesamientos de datos personales pueden ser de tipo descriptivo o prescriptivo. Son descriptivos cuando están encaminados a segmentar o a perfilar a los usuarios, de acuerdo con una categorización de sus datos personales a partir de sus intereses, gustos o hábitos. Son prescriptivos cuando su objetivo está orientado a predecir o a inducir el comportamiento del titular de los datos personales. En general, las políticas de privacidad de la EMNBD no indican

8 Para más información, ver la sección de "Aplicaciones, sitios web e integraciones de terceros en nuestros Productos o que usan nuestros Productos" de las políticas de privacidad de Facebook en https://es-es.facebook.com/privacy/explanation

las tecnologías o los métodos de *big data* utilizados para llevar a cabo tratamientos de esta estirpe.

Ninguna compañía analizada en México especifica esta cuestión. En Chile, Facebook y Falabella se limitan a indicar que realizan análisis de datos con el fin de segmentar a los usuarios para personalizar el contenido, mas no indican de qué manera realizan dicho análisis. Las políticas de privacidad de algunas de las EMNBD analizadas en Colombia y Brasil tienen un mayor nivel de detalle, aunque no el deseable. Microsoft, Netflix, Google, Social Miner y AliExpress indican que el análisis se hace por medio de procesos automatizados, *machine learning*, algoritmos o sistemas como Google Analytics. Estos conceptos, debe decirse, son sumamente amplios e indeterminados. Aunque es un avance en comparación con aquellas empresas que no incluyen información al respecto, indicar el uso de sistemas automáticos, algoritmos o *machine learning* realmente no permite que las personas del común —ni tampoco los expertos— conozcan qué sucede con sus datos y cómo se adelanta su tratamiento.

A la falta de transparencia o especificidad de las políticas de privacidad estudiadas, en relación con los métodos por medio de los cuales las EMNBD analizan datos personales, se suma el silencio legal en la materia. En ninguno de los países objeto de estudio las normas de protección de datos obligan a que el responsable del tratamiento de datos personales indique claramente la tecnología que usa para procesar la información. Una precisión de la normativa en este punto es de la mayor importancia: permitiría que los usuarios se hagan una idea de qué sucede con sus datos personales una vez entregados o recolectados, y de contera, permitiría garantizar la aspiración del consentimiento libre e informado que es el que en últimas legitima todo proceso de tratamiento de datos personales en el sector privado.

1.3. Finalidades del tratamiento de datos personales

El tratamiento de datos personales por parte de las EMNBD analizadas persigue, por lo general, dos grandes objetivos. Por un lado, prestar adecuadamente el servicio y, por ende, mejorar la experiencia del usuario/cliente, ofrecer nuevos productos o servicios y realizar investigación de mercado. Por el otro, compartir esta información, o los productos de esta información, con terceros.

Por lo general, las políticas de privacidad estudiadas son bastante claras en cuanto a las finalidades que persiguen con el tratamiento de datos. En ese sentido, empresas como Falabella (Chile), Telcel (México) o Magazine Luiza (Brasil) incluyen en su política de privacidad listados fáciles de entender en relación con los propósitos del tratamiento. Telcel y Payclip en México establecen que hay finalidades primarias —que son esenciales para proporcionar el servicio— y secundarias —aquellas que el usuario puede decidir no consentir y, que, por tanto, permiten excluir sus datos para tales tratamientos—. Las finalidades primarias coinciden con el objeto de la EMNBD y, por tanto, son necesarias para la prestación del servicio o para la ejecución de la función de la plataforma (prestar el servicio de telefonía, permitir la facturación, concretar la entrega del producto en el domicilio, etc.). Las finalidades secundarias están relacionadas con la comunicación con el cliente para la ampliación de los servicios o la celebración de nuevos contratos (envío de publicidad, informes sobre la empresa, cesión a terceros para ciertos fines, etc.).

Ahora bien, no todas las EMNBD cumplen con estos estándares de transparencia. AIRA, en Chile, se limita a indicar que utilizará la información recolectada únicamente en relación con los servicios prestados. Amazon, por su parte, indica de manera ilustrativa, mas no taxativa, algunas de las finalidades con las que realiza el tratamiento de datos, dejando la puerta abierta a que existan más. La falta de claridad se debe también a la dificultad que puede tener un usuario para encontrar la información. El caso de Facebook es notable porque no tiene un listado único de finalidades, sino que estas se encuentran dispersas a lo largo de toda su política de privacidad, dependiendo del tema que se trate en cada apartado. Esta práctica dificulta que un usuario obtenga de manera directa y sencilla la información que necesita sobre las finalidades para las que Facebook hace uso de sus datos.

2. Las legislaciones de protección de datos de Brasil, Chile, Colombia y México

El análisis de la legislación en materia de protección de datos determina qué tan preparado está un ordenamiento jurídico para enfrentar los retos de la era digital. Según las conclusiones de los informes de los cuatro países estudiados, las legislaciones locales no son suficientes para regular las dinámicas de acopio y tratamiento de datos de las EMNBD. En esta

sección presentaremos los aspectos comunes que condicionan el nivel de preparación de la normativa de Brasil, Chile, Colombia y México para hacer frente a las prácticas de tratamiento de datos propias de la economía digital. Para esto, nos concentraremos en tres temas: 1) el ámbito de aplicación de la ley nacional, 2) la (in)adecuación de la legislación para enfrentar fenómenos propios de la era digital y 3) las capacidades/competencias de la autoridad de protección de datos.

2.1. Ámbito de aplicación de la ley

Siguiendo el principio general del derecho sobre aplicación territorial de la ley, las legislaciones de protección de datos de Chile, Colombia y México son aplicables, casi exclusivamente, cuando el tratamiento de datos personales sea realizado en el país y por responsables domiciliados en el territorio nacional[9]. La legislación mexicana, sin embargo, incluye un supuesto adicional: cuando el responsable del tratamiento "no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen con fines de tránsito que no impliquen un tratamiento". En Colombia, por ejemplo, el Artículo 2° de la Ley 1581 de 2012, indica que dicha normativa también será aplicable cuando al responsable del tratamiento "no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".

2.1.1. El domicilio de la EMNBD como criterio para la aplicación territorial de la ley

Las legislaciones de Chile, Colombia y México se aplican, en principio, a responsables del tratamiento que se encuentren efectivamente domiciliados dentro de la jurisdicción territorial del Estado. Lo anterior se desprende tanto de una interpretación literal del texto legal —o, mejor dicho, de su silencio al respecto— como, en parte, de la práctica judicial. En México, el INAI ha interpretado que la legislación de protección de datos no le es aplicable a personas domiciliadas en otros países. Esta

9 Según el Artículo 2° de la Ley 1581 de 2012 (Colombia) y el Artículo 4° del Reglamento de la LFPDPPP (México), la normativa nacional será aplicable cuando el tratamiento sea realizado dentro del territorio o cuando el responsable del tratamiento no se encuentre en el territorio nacional, pero le sea aplicable su legislación en virtud de convenios o tratados internacionales.

situación pone de presente uno de los mayores retos a los que se enfrenta la regulación sobre estos asuntos en América Latina. En razón a que el criterio para la aplicación de la ley es el lugar en el cual se realice el tratamiento o en el que se encuentre domiciliado el responsable, la ley de ese lugar no le sería aplicable a las grandes empresas de internet como Google, Apple, Facebook, Amazon o Microsoft. Estas empresas, por lo general, se encuentran domiciliadas en Estados Unidos y tienen oficinas —no está claro si se trata de filiales— alrededor del mundo.

En efecto, desde 2019 la autoridad de protección de datos colombiana ha considerado que la ley colombiana es aplicable a empresas transnacionales que recolecten datos de personas que residan en el territorio nacional, toda vez que la recolección hace parte del tratamiento y, por ende, es posible considerar que el tratamiento se realiza en el territorio del Estado. En desarrollo de esta interpretación, esta autoridad ha expedido sendas resoluciones en las que instruye la protección de datos personales de nacionales colombianos a empresas sin domicilio en Colombia: Facebook y Uber[10].

En contraste, en Chile, la Ley Nº 19.628 no se refiere en absoluto a su ámbito de aplicación. Esto ha llevado a que, en la práctica, su interpretación sea acotada, en cumplimiento de los principios generales del derecho. Por tal motivo, aunque no exista disposición expresa sobre el particular, la Ley Nº 19.628 es aplicable únicamente respecto del tratamiento de datos personales que tenga lugar al interior del territorio chileno. Resulta extraño que el proyecto de ley que se tramita en el Congreso chileno no contenga disposiciones especiales sobre la aplicación territorial de la ley, un aspecto crítico frente a los actores y las prácticas de tratamiento de la era digital. Como mucho, este proyecto obliga a que el responsable que no tenga domicilio en el territorio, pero realice tratamiento de datos de personas nacionales, disponga de un buzón de contacto, con una cuenta de correo electrónico habilitada para los efectos.

---

10 Al respecto, véase la Resolución 1321 de 2019 (caso Facebook) y la Resolución 21478 de 2019 (caso Uber) de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio. Ambas decisiones fueron apeladas. Sin embargo, en el caso Facebook la decisión de segunda instancia confirma la decisión de primera instancia. Al momento de publicación de este documento todavía no se ha resuelto la segunda instancia del caso Uber.

2.1.2. El domicilio del titular de los datos como criterio para la aplicación territorial de la ley

A partir de la entrada en vigencia Reglamento General de Protección de Datos de la Unión Europea (GDPR, por sus siglas en inglés) el ámbito de aplicación territorial de la regulación de protección de datos europea ya no depende del lugar en el que se encuentre el responsable del tratamiento, sino del lugar en el que se encuentre el titular de los datos personales objeto de tratamiento. Según el Artículo 3 del GDPR, este se aplica:

> al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: la oferta de bienes o servicios a dichos interesados en la Unión [...] o el control de su comportamiento.

Esto quiere decir que la normativa europea debe ser acatada por empresas transnacionales como GAFAM, incluso si no tienen domicilio en Europa, siempre que el tratamiento de datos personales se relacione, *grosso modo*, con situaciones propias de la economía digital.

Inspirándose en el GDPR, la Ley Nº 13.709 de 2018 de Brasil establece en su Artículo 3º que la normativa nacional es aplicable en los siguientes escenarios: 1) cuando el tratamiento sea realizado en Brasil, 2) cuando el tratamiento tenga como objeto la oferta de bienes y servicios y 3) cuando los datos personales objeto de tratamiento hayan sido recogidos en territorio nacional —mejor dicho, cuando el titular de los datos personales se encuentre en Brasil—. La ley brasileña entrará en vigencia a mediados del año 2020, por lo que para la fecha de terminación de este reporte no existen datos que den cuenta de su nivel de eficacia.

Por otra parte, la interpretación que ha sostenido recientemente la Autoridad de protección de datos personales colombiana, sobre el ámbito de aplicación de la ley, es muy similar a lo dispuesto en el GDPR y en la normativa brasileña. Según esta autoridad, las empresas transnacionales deben cumplir con la legislación colombiana porque realizan tratamiento (es decir, recolección) de datos personales en Colombia. Es importante aclarar que Facebook y Uber apelaron las decisiones, por considerar que la ley de protección de datos colombiana no les es aplicable, y hasta el momento de cerrar la edición de este informe, en segunda instancia, la autoridad de protección de datos en Colombia, un órgano de naturaleza

típicamente administrativa, había confirmado la decisión condenatoria en el caso contra Facebook.

2.2. Regulación inadecuada o insuficiente para la era digital

De las normativas existentes en los países estudiados, la que más se ajusta a las nuevas prácticas y a las vicisitudes técnicas propias de la era digital es la legislación brasileña (Ley Nº 13.709 de 2018). Las legislaciones de los otros países analizados (Chile 1999, México 2010, Colombia 2012) son indiferentes —en el mejor de los casos siguiendo el principio de neutralidad tecnológica— al lenguaje y a las particularidades de las prácticas digitales del siglo XXI. A pesar de que sus términos, generales y abstractos, permiten una paulatina adecuación interpretativa a las complejas prácticas de tratamiento de datos personales propios de la economía digital, los estudios aquí referenciados dan cuenta de la conveniencia de adecuar dichas regulaciones, o de adecuar su interpretación, para hacer frente, entre otros, a los problemas relacionados con el *web tracking*, la identificación de datos personales a partir de acumulación y relacionamiento (datos personales inferidos), el perfilamiento, la analítica predictiva, la toma de decisiones automatizadas, el derecho al acceso efectivo de la información personal, y el derecho a la oposición de tratamiento, entre otros.

2.2.1. Web tracking, *IP y la definición de 'dato personal'*

Uno de los elementos comunes a las legislaciones de Brasil, Chile, Colombia y México es que no está claro cuál es el estatus jurídico de los datos recolectados por medio del monitoreo o *web tracking*. Lo anterior es problemático porque las EMNBD, como hemos visto (en los casos de las brasileñas iFood y Social Miner, por ejemplo), consideran que la información que obtienen por medio de esta práctica no constituye información personal —se trataría de información estadística, por ejemplo— y, en consecuencia, estiman que no les es aplicable la legislación sobre protección de datos.

La definición de dato personal de las legislaciones de los países estudiados es maximalista y utiliza universales positivos[11], lo cual, sin

11 Según el literal c) del Artículo 3º de la Ley 1581 de 2012, en Colombia un dato personal es aquella información "vinculada o que pueda asociarse a

duda, facilita las adecuaciones interpretativas. Sin embargo, ante la sofisticación de las prácticas de recogida de datos, en contextos altamente tecnificados, las siguientes preguntas son pertinentes: ¿la información sobre el dispositivo, el navegador utilizado y el historial de búsqueda generado a partir de cierto aparato constituye dato personal? ¿La información sobre el protocolo de internet (IP) de un dispositivo —que permite identificar cualquier dispositivo y el lugar del mundo en el que se conectó a internet— es un dato personal? ¿Esto independientemente de que tales aparatos o dispositivos sean empleados por diferentes personas?

No existe en las legislaciones de los países estudiados disposición que estime, de forma explícita, los identificadores en línea o las interacciones entre dispositivos y plataformas como dato personal. Estos son elementos básicos de las interacciones en internet y fundamentales en la operación de la EMNBD. Con el fin de evitar esta incertidumbre jurídica, los legisladores en Europa y California optaron por incluir dentro de la definición de dato personal aquella información que puede ser recolectada por medio de *web tracking* y que usualmente está relacionada con nuestros dispositivos[12]. Esto elimina la posibilidad de que la captura y el tratamiento de esta información, por parte de las EMNBD, suceda

una o varias personas naturales determinadas o determinables". En Chile, el literal f) del Artículo 2° de la Ley N° 19.628 establece que los datos personales son aquellos "relativos a cualquier información concerniente a personas naturales identificadas o identificables". De igual manera, la legislación mexicana define los datos personales como "información concerniente a una persona física identificada o identificable" (LFPDPPP, Artículo 3, numeral V). Por su parte, la Ley General de Protección de Datos de Brasil define los datos personales como la "información relacionada a una persona natural identificada o identificable".

12 En ese sentido, el CCPA en su sección 1798.140 establece que dentro del concepto de información personal se encuentran, de manera ilustrativa mas no taxativa, los protocolos de identificación de internet (IP), el correo electrónico, los datos de geolocalización, la actividad web de las personas, su historial de navegación y cualquier otra interacción del consumidor con un sitio de internet o aplicación móvil. El GDPR, en contraste, reconoce en su considerando 30 que "las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos". Así, al definir el concepto de datos personales como toda información sobre una persona física identificada o identificable, indica que "se considerará persona física identificable toda persona cuya identidad pueda determinarse [...] en particular mediante [...] datos de localización [o] un identificador en línea" (GDPR, Artículo 4, numeral 1).

sin posibilidad alguna de control. También sirve de muestra de cómo la normativa de protección de datos personales puede cumplir mejor su función, si se encuentra ajustada a las exigencias de la era digital y reconoce que dentro de las dinámicas de la economía digital se encuentra la explotación a gran escala de datos recolectados por medio de las interacciones en internet.

2.2.2. Cookies y transparencia

Al igual que sucede con otras herramientas tecnológicas que facilitan la recolección de información, las legislaciones de Brasil, Chile, Colombia y México no hacen referencia al uso de *cookies* u otro tipo de tecnología por medio de la cual se realiza *web tracking*. Tampoco regulan qué tan clara y entendible debe ser la información al respecto. ¿Resulta suficiente —y comprensible para un usuario medio— indicar que la aplicación o página web utiliza *cookies* para recolectar información? ¿No sería recomendable que, en el contexto de las obligaciones de transparencia y de finalidad y propósito, se incluyeran a nivel legal o interpretativo subreglas en materia de *cookies*? Estas preguntas cobran mayor relevancia cuando se trata de la recolección de datos sensibles. Por ejemplo, en Chile, los hábitos personales, dentro de los cuales se encuentra la actividad reiterada de una persona en la web, son considerados datos sensibles y, por ende, tienen mayor grado de protección. Sin embargo, ante la inadecuación técnica de la regulación de protección de datos a la era digital, se diluye la posibilidad de mayores controles sobre el uso de *cookies*. Ni siquiera la legislación brasileña expedida en 2018 tiene previsiones específicas sobre esta materia, lo cual resulta, cuando menos, sorprendente.

2.2.3. Los datos sensibles inferidos

Los ordenamientos jurídicos estudiados enfrentan el reto de cómo regular las prácticas de tratamiento (acopio-obtención-identificación) de datos inferidos, y en especial de datos sensibles inferidos y de datos utilizados para inferir dichos datos. Gracias a los desarrollos de técnicas de minería de datos y de análisis de *big data*, las EMNBD pueden inferir datos de las personas sin que estas los hayan entregado de manera directa y voluntaria. Estas prácticas de inferencia de datos personales permiten precisar y explicitar nuevas informaciones que, una vez 'producidas' tengan la calidad de datos sensibles.

Existe relativo acuerdo sobre la prohibición, salvo algunas excepciones, del tratamiento de datos sensibles, y sobre los especiales deberes de salvaguarda y de tratamiento de este tipo específico de información personal. Esta prohibición y estos deberes, sin embargo, resultan inaplicables en la práctica, porque las EMNBD pueden hacerse a la información —o acercarse bastante a ella— por medio de la inferencia de datos. Mediante análisis de conjuntos de datos no sensibles (supongamos, historial de búsqueda, compras, etc.) pueden inferirse datos sensibles (sexo/género, orientación sexual, ideología política, salud, creencias religiosas, etc.). Lo que se desprende de este estudio es que distintas EMNBD realizan tratamiento efectivo de estos datos en un aparente escenario de anomia. Ello es así porque no existe disposición legal que regule la obtención y el tratamiento de datos sensibles por la vía de la analítica de datos o de procesos de inferencia y relacionamiento de datos.

2.2.4. El perfilamiento

Otro de los aspectos no regulados por las legislaciones estudiadas es la creación de perfiles (o perfilamiento) de los usuarios con cualquier fin, siendo la toma de decisiones automatizadas de carácter comercial (*marketing)* el uso más común. El perfilamiento automatizado es posible gracias al *big data,* el cruce y la minería de datos. Así, gran cantidad de información es analizada y sistematizada para identificar a cada quien por medio de distintas y numerosas unidades de información (*data points*) que, al ser recolectadas masivamente, relacionadas y puestas en contexto pueden decir algo (o mucho) de una persona. Esta situación no es menor. El perfil virtual de una persona física, creado por una EMNBD, suele ser empleado para determinar los servicios a los que tiene acceso y los productos que puede adquirir, o para incidir en los derechos que le son garantizados, en la información que se le muestra, y en la decisión de ser objeto o no de vigilancia activa (Büchi, Fosch-Villaronga, Lutz, Tamò-Larrieux, Velidi y Viljoen 2019).

Si bien las EMNBD por lo general hacen perfilamiento de sus usuarios con fines comerciales, como los de ofrecer publicidad dirigida y dar acceso a ciertos bienes o servicios, lo cierto es que esta práctica corporativa no está exenta de riesgos, especialmente de aquellos asociados con la modificación del comportamiento online de las personas (Marder, Joinson, Shankar y Houghton 2016). Hay autores que afirman que los usuarios cambian sus hábitos de navegación intentando anticipar las decisiones

automatizadas producto del perfilamiento (Gräf 2017), lo cual supone riesgos todavía inexplorados para la autonomía individual (Kandias, Mitrou, Stavrou y Gritzalis. 2016). La inexistencia de regulación sobre la forma en la que se pueden realizar perfiles, o sobre las decisiones automatizadas basadas en ellos, deja a los usuarios en total desventaja frente al poder de acción y decisión de las EMNBD.

2.2.5. Respuesta regulatoria al perfilamiento

Advertidos de los riesgos anteriores, el europeo GDPR establece la obligación de informar a los usuarios cuándo serán objeto de decisiones automatizadas y de perfilamiento. Esta obligación incluye el deber de informar sobre la lógica aplicada —es decir, cómo funciona el sistema— y las consecuencias que puede tener para las personas (literal f, numeral 1, Artículo 7). Asimismo, esta normativa indica que las personas podrán oponerse al tratamiento de datos personales cuando este implique la elaboración de perfiles o la toma de decisiones automatizadas que los afecte significativamente (numeral 1, Artículo 21). Es importante resaltar que el proyecto de ley que se tramita en el Congreso chileno recoge algunas de estas lecciones e incluye una definición sobre la creación de perfiles. Las legislaciones de Brasil, Colombia y México guardan silencio al respecto, lo que deja nuevamente sin protección específica al titular de los datos personales.

2.2.6. El derecho de oposición

El derecho de oposición faculta al titular de los datos personales para recuperar el control sobre su información personal e inhibir actividades de tratamiento en caso de que estas sean ilegales o ilegítimas. Sin embargo, la inexistencia de este derecho en las regulaciones de Chile y Colombia, y su probada poca eficacia en México, es otra de las carencias regulatorias (¿o interpretativas?) identificadas en el presente estudio. Por ejemplo, todas las políticas de privacidad de las l analizadas en Colombia deben ser aceptadas o rechazadas en bloque, sin otorgar la posibilidad de que una persona se oponga al tratamiento de datos personales de cierta manera o para determinado fin, desde el inicio o durante las fases posteriores al tratamiento. De igual forma, la ley mexicana no ofrece mecanismos para excluir de la autorización de uso de datos, la toma de decisiones automatizadas o la creación de perfiles. Este derecho (también conocido como *right to opt out*) permitiría que los usuarios tengan mayor control

sobre sus datos personales. No en vano, tanto la normativa europea como el ccpa —en lo relacionado con la comercialización de datos (sección 1798.129)— permiten que los usuarios se opongan al tratamiento de datos personales de cierta forma y entreguen parcialmente su consentimiento.

2.3. Capacidades de la autoridad de protección de datos

No todos los ordenamientos jurídicos contemplan la existencia de una autoridad encargada de la protección de datos personales. Sin embargo, en Brasil, Colombia y México existe una autoridad nacional de protección de datos y en Chile está en marcha el proceso para su creación. Esto parece dar cuenta de la importancia que tiene la existencia de una autoridad de protección de datos personales para garantizar adecuadamente los derechos fundamentales de las personas en un contexto de tratamiento de datos masivo e intensivo.

2.3.1. La extensión de la competencia y el problema de la territorialidad

La competencia de las autoridades de protección de datos depende, en gran medida, del ámbito de aplicación de la normativa de protección de datos. En Chile, Colombia y México la ley no parece reconocer de forma explícita su competencia para adelantar actividades de control y vigilancia sobre las EMNBD que no se encuentren domiciliadas en territorio nacional o cuyo tratamiento de datos personales se adelante en otro país. Esto, como lo hemos visto, podría suponer que la autoridad de protección de datos, al menos en principio, carece de competencia para pronunciarse sobre el tratamiento de datos realizado por empresas como Facebook o Google, incluso si los datos pertenecen a nacionales colombianos o mexicanos.

Sin embargo, en el año 2015, la autoridad de protección de datos mexicana expidió una resolución contra Google en un caso relacionado con el derecho de oposición de un titular de datos personales mexicano. Esta decisión fue anulada posteriormente en sede judicial, y el caso se encuentra todavía pendiente. Por su parte, en 2019, la autoridad de protección de datos colombiana ha buscado por vía interpretativa extender su potestad de vigilancia y control para cobijar EMNBD domiciliadas en otros países, pero que adelantan prácticas de recolección de datos en territorio nacional, sin que todavía este criterio haya superado el control judicial de legalidad.

A pesar de estos valiosos esfuerzos interpretativos, el fortalecimiento de las capacidades de actuación de estas autoridades depende, entre otras, de que todos los actores institucionales interpreten adecuadamente el ámbito de aplicación de forma amplia. Esto permitiría precisar la competencia de la autoridad de protección de datos sobre las EMNBD que adelanten cualquier tipo de tratamiento sobre los datos personales de los nacionales del Estado respectivo. En este sentido, es aconsejable una modificación explícita de las leyes o una interpretación integral que se ajuste a la realidad digital. Una posible alternativa regulatoria puede ser la tomada por los Estándares Iberoamericanos (consideración 22), el GDPR y por la normativa brasileña, cuyo factor determinante es la residencia del titular de los datos que son objeto de tratamiento. Esto puede lograrse mediante la modificación de las legislaciones locales o por medio de interpretaciones amplias de la norma existente o, en un escenario ideal, mediante la aprobación de un tratado internacional regional en la materia.

2.3.2. Las capacidades institucionales

Más allá de la dificultad de hacer rendir cuentas a empresas transnacionales, las autoridades de protección de datos analizadas tienen una capacidad limitada para hacer frente a las dinámicas propias de la era digital. Esto es así, al menos, por dos razones. En primer lugar, porque la garantía de este derecho hace necesario que quienes trabajen en la autoridad de protección de datos tengan amplio conocimiento en dos áreas complementarias: 1) ciencias de la computación, es decir, nociones básicas de cómo funcionan internet, el mercado de datos, el *machine learning*, la inteligencia artificial, el *big data*, los algoritmos, etc.; y 2) ciencias jurídicas, especialmente en lo relacionado con comercio electrónico, propiedad intelectual, derecho a la protección de datos y derechos humanos en la era digital.

En segundo lugar, los requisitos procesales para provocar pronunciamientos, distintas barreras de entrada y la ausencia de personal o de personal calificado, impiden que la autoridad sea eficiente en su función. Tanto el INAI en México, como la Delegatura para la Protección de Datos Personales en Colombia, tienen resultados magros en relación con la atención y resolución de solicitudes y/o quejas de titulares de datos personales. En México, por ejemplo, en 2018 únicamente se presentaron 251 solicitudes de Procedimiento de Protección de Derechos ante

el INAI (en los que no necesariamente estaba involucrada una EMNBD). De todos estos, menos de 25 resultaron en la modificación y/o arreglo de la situación. Este dato es indicativo del muy reducido número de solicitudes elevadas ante el INAI, frente a la población total de México (aproximadamente 120 millones de personas) y también es indicativo del relativamente bajo índice de éxito que tiene dicho procedimiento.

En Colombia, en contraste, la Delegatura para la Protección de Datos Personales de la SIC recibe un número elevado de reclamos al año. Según estadísticas disponibles en su página web, en 2016 se encontraban en trámite 2230 denuncias por protección de datos personales. En ese mismo año, la Delegatura impartió casi 400 órdenes o multas para remediar la afectación a derechos. Sin embargo, el número de procesos que llegan es mucho mayor a la capacidad que tiene para resolverlos, lo que supone un largo tiempo de espera[13]. No obstante, desde 2018 ha habido un aumento sustancial en el número de funcionarios que trabajan en la autoridad de protección de datos, lo que puede suponer un aumento en su eficacia. En ese sentido, según la misma entidad, en 2019 se impartieron casi mil órdenes o multas y se expidieron tres guías sobre temas de actualidad: comercio electrónico, transferencias internacionales de datos y marketing y publicidad. Lo anterior demuestra un aumento sustancial en las capacidades de la Delegatura para la Protección de Datos Personales en Colombia.

2.3.3. Diseño institucional

El diseño institucional de la autoridad de protección de datos es un asunto capital. En especial, si este apunta a favorecer su independencia de los poderes públicos, pero también de los poderes privados.

En México está clara la autonomía técnica y presupuestal del INAI y se predica su carácter independiente, desde su caracterización como órgano constitucional autónomo, y su integración por 7 comisionados elegidos por el Senado de la República. Frente al que podría considerarse un diseño institucional adecuado están los casos de Colombia y Brasil.

En el caso colombiano, a pesar de gozar de cierta autonomía técnica y presupuestal, la autoridad de protección de datos es un delegado del

---

13 Indicadores por proceso de 2015 sobre la Vigilancia Administrativa de Protección de Datos Personales. Datos Estadísticos–Gestión Institucional, en el que se desglosan las actividades de la SIC desde 2013 hasta 2016.

presidente de la República, y la Delegatura para la protección de datos personales es una oficina más dentro de la Superintendencia de Industria y Comercio, la oficina del Gobierno nacional mediante la cual este descarga sus funciones constitucionales de inspección y vigilancia de las actividades industriales y comerciales que se adelantan en el país.

Una situación similar ocurre en Brasil en donde, la *Autoridade Nacional Proteção de Dados Pessoais* es dependiente de la Casa Civil de la Presidencia de la República. Dentro de la estructura institucional, la mencionada autoridad se encuentra inserta en el poder Ejecutivo y está sujeta a su voluntad. De hecho, fue la presidencia quien propuso este arreglo institucional; esta se opuso a que fuera el Congreso el órgano encargado de legislar en la materia, en tanto consideraba que se trataba de un tema de competencia exclusiva de la Presidencia, al guardar relación con la organización de la administración pública. Por tal motivo, la autoridad de protección de datos en Brasil no cuenta con autonomía presupuestal, ni con total libertad para trazar su agenda, lo que supone un arreglo institucional desafortunado a la hora de garantizar adecuadamente el derecho a la protección de datos de las personas.

Por último, no tenemos certeza sobre la suerte que correrá la creación de la agencia de protección de datos chilena y si tendrá independencia total de otros poderes políticos. Es importante mencionar que la definición del carácter y del lugar de esta autoridad en el contexto institucional chileno es producto de una pugna de poder entre el Ejecutivo y el Legislativo. Fue apenas en agosto de 2019 que el Senado confirmó que acogería la propuesta del Ejecutivo, según la cual el Consejo para la Transparencia se transformaría en la nueva autoridad nacional de protección de datos. Aunque este Consejo ha gozado hasta ahora de cierta autonomía, no es seguro que siga siendo así, sobre todo por cuestiones presupuestales y de capacidad institucional.

Conclusiones y recomendaciones

Las EMNBD analizadas en Brasil, Chile, Colombia y México realizan acopio y tratamiento de datos personales en el novedoso contexto de la era digital y mediante herramientas tecnológicas especiales y en constante transformación. La diversidad de las estrategias de negocio y de los objetos sociales de las EMNBD se traslada a sus políticas de privacidad. Estas, a su vez, expresan la concepción del negocio y los valores

empresariales en relación con las prácticas de acopio y tratamiento de los datos personales. En general, las EMNBD estudiadas, sobre todo las arraigadas en una jurisdicción territorial específica, intentan ajustar sus prácticas a la legislación local.

Sin embargo, el especial protagonismo de las GAFAM y su doble característica de gigantes de internet y de empresas foráneas (todas con domicilio principal en los EE.UU.) revela ciertas perplejidades sobre la adecuación de las prácticas de acopio y tratamiento de datos personales, con los términos y exigencias de las legislaciones locales. A esta situación, se suma la versatilidad de las prácticas de acopio y tratamiento, en un escenario especialmente cambiante, y la constante novedad de las tecnologías dispuestas para ello. Desde las sofisticadas prácticas de *web tracking*, hasta el refinamiento de las herramientas para adelantar analítica de datos, en un escenario de concentración masiva de datos y de fabulosas capacidades de almacenamiento y de procesamiento de la información personal.

Los estudios analizados revelan además el creciente protagonismo de las GAFAM en el entorno de la economía digital, también revelan, por obvias razones temporales, que las legislaciones estatales, en especial las de Chile, Colombia y México, se encuentran desfasadas o que, por lo menos, su interpretación actual es insuficiente. A pesar de que, en ocasiones, los estudios reconocen la posibilidad de adaptar o interpretar las disposiciones vigentes para regular estas 'nuevas' prácticas, también indican la pertinencia, cuando no la necesidad de adecuar la legislación para hacerle frente a estas nuevas situaciones, y poder así cumplir la promesa de la eficacia del derecho fundamental a la protección de datos en la era digital.

El ejercicio comparativo de los estudios aquí recogidos nos ha revelado la existencia de, al menos, tres grandes tipos de problemas en atención a las prácticas de acopio y de tratamiento de las EMNBD en la era digital. El primero, relacionado con la transparencia y con el consentimiento. El segundo, relacionado con la necesidad de adaptar la legislación a las prácticas específicas de las tecnologías que soportan el esquema de negocios de las EMNBD. Y el tercero relacionado con las garantías del derecho fundamental a la protección de datos personales.

El problema de la transparencia es acuciante. Las prácticas de acopio y de tratamiento de datos personales son altamente sofisticadas. El acopio se produce por diversas vías y no solo directamente de la fuente

mediante procesos más o menos claros de registro. El *web tracking* y el uso de distintos mecanismos para compartir información, como los botones de las redes sociales, Facebook en especial, o el uso de Google Analytics, no es suficientemente claro ni explícito. Son extraordinarias las políticas de privacidad que describen con detalle el tipo de datos personales objeto de recogida, o que explican con detalle las complejas interacciones entre distintos agentes que, por una u otra vía, terminan en posesión de los datos personales de los nacionales de los Estados bajo estudio. La demanda de transparencia se enfrenta, por otra parte, a que la información relativa al tratamiento, contenida en dichas políticas de privacidad, se encuentra en un lenguaje altamente técnico, o está disperso en varios documentos, o está escrito solo en un idioma que no es el oficial del país en donde sucede la recogida de los datos personales, o que simplemente está contenido en textos planos y muy extensos. Todo esto, en perjuicio de una idea básica: que las personas del común entiendan o estén en condiciones de entender cuáles de sus datos son recogidos, para qué finalidad serán objeto de tratamiento, con qué efectos e implicaciones y por cuánto tiempo.

Por otra parte, los problemas asociados con la falta de regulación específica, que atienda la complejidad técnica de las prácticas de acopio y tratamiento, merecen especial atención por los actores relevantes (legisladores, autoridades nacionales de protección de datos, académicos, agentes y activistas). Deberían ser objeto de regulaciones explícitas, por lo menos, las prácticas de *web tracking*, el uso intensivo de *cookies* de distinto tipo, las posibilidades de identificar datos por inferencia o por relacionamiento, las prácticas de perfilamiento con distintos fines, el uso de distintas herramientas de cruce, analítica y minería de datos, el uso de complejos algoritmos y, a partir de aquí, la sofisticación de las prácticas de marketing digital, de microtargeting, de analítica predictiva y de toma de decisiones automatizadas con capacidad de afectar a los titulares de los datos.

En esta última hipótesis, considérense, por ejemplo, los casos de presentación de publicidad de ciertos productos (en apariencia el más anodino), hasta los más delicados como la construcción de burbujas informativas, o de inducción explícita o subliminal para la toma de decisiones individuales. Los estudios aquí analizados dan cuenta de las limitaciones de las legislaciones en la materia en cuestiones, si se quiere hoy, elementales: la definición del carácter de la IP como un dato personal,

la existencia de diferentes *cookies* y la necesidad de que los titulares de datos puedan controlar el tipo de información personal que estas pueden capturar, o la necesidad de proteger las libertades de las personas frente a la multiplicación de las decisiones automatizadas.

Finalmente, los estudios también revelan la insuficiencia de las garantías del derecho a la protección de datos en la era digital, y en el contexto crítico de la operación de las EMNBD y su relación con GAFAM. No solo por el problema de la aplicación extraterritorial de la ley local, que quizá sea uno de los grandes problemas que enfrentamos como región, sino también por los problemas relacionados con la definición y el alcance de los derechos de participación en los procesos de acopio y tratamiento, y en especial por el alcance del derecho de oposición. Esto es, del derecho a que el titular de los datos reclame su titularidad y pueda oponerse, con éxito, al tratamiento de sus datos personales una vez se advierta que es ilegal o ilegítimo.

Sin embargo, a pesar de que este derecho sea reconocido y afirmado como tal por las legislaciones locales, faltarían las condiciones institucionales para garantizarlo: procesos judiciales efectivos y céleres tipo amparo no son la regla en las regulaciones estudiadas, y las capacidades institucionales de las autoridades de protección de datos personales han sido puestas en duda. En unos casos, por las dificultades para articular los procedimientos administrativos y las limitaciones propias de los órdenes legales internos (México, Colombia); en otros, porque las multas no son suficientemente disuasorias (Chile), y en los demás, por ausencia de independencia o de voluntad política (Brasil) y, en general, por la precariedad de las capacidades técnicas y operativas, y por el claro desbalance de poder existente entre las autoridades de protección de datos y los sujetos de control (GAFAM).

Los problemas de transparencia efectiva, las deficiencias regulatorias y la ausencia de garantías efectivas son una mala noticia para el titular de los datos personales en la era digital. Este diagnóstico agrava la relación desigual de poder entre los titulares de datos y las EMNBD, y en especial entre aquellos y GAFAM. Asimismo, no todas las leyes nacionales (o la interpretación dominante en cada país) son aplicables al tratamiento de datos personales que realizan empresas transnacionales como Google o Facebook.

A partir de esta(s) conclusión(es), proponemos las siguientes recomendaciones, inspiradas en el doble propósito de balancear la relación de

poder entre las EMNBD y los titulares de datos personales, y de avanzar la agenda de la garantía, y ojalá de la eficacia, del derecho fundamental a la protección de datos de los usuarios digitales:

1. Establecer el principio de transparencia como guía para las políticas de privacidad (o términos de servicio) con el fin de informar adecuadamente cómo y con qué fines se realiza el acopio y el tratamiento de datos personales. En especial, en relación con: 1) la cesión, por cualquier forma, de datos entre aplicaciones o EMNBD; 2) la relación comercial y/o de colaboración entre las aplicaciones y GAFAM; 3) la creación de perfiles de los usuarios con fines publicitarios o comerciales y 4) la toma de decisiones automatizadas basándose en dichos perfiles o en la actividad de los titulares de datos personales.
2. Adaptar las legislaciones locales o su interpretación al entorno digital. En especial, en relación con: 1) la recolección de datos por medio de *web tracking*, *cookies* y otras herramientas digitales, 2) la inclusión dentro del concepto de 'dato personal' de información relativa a los dispositivos como la dirección IP, el historial de navegación y de búsqueda, y la geolocalización, 3) la regulación de las prácticas de inferencia de datos, perfilamiento y decisiones automatizadas.
3. Reconocer, de forma efectiva, en clave de *habeas data* el derecho de oposición de los titulares de datos personales a ciertos tipos de tratamiento y en relación con temas específicos (comercialización de datos, decisiones automatizadas, creación de perfiles, etc.), sin que esto termine condicionado a la prestación o no del servicio.
4. En los países en los que aún no es así, extender el ámbito de aplicación de la legislación nacional para que comprenda el tratamiento de datos personales por empresas sin domicilio en el país, a la vez que se reconozca de forma explícita la competencia de las autoridades locales de protección de datos. Sobre este punto podría acogerse la propuesta de los Estándares Iberoamericanos, del GDPR y de la legislación brasileña o de la autoridad de protección de datos colombiana, de tomar el lugar de residencia del titular de los datos personales, o el lugar

de la recogida de los datos, como criterios de aplicación de la legislación de protección de datos personales.

5. Fortalecer las capacidades —tanto tecnológicas como jurídicas—, la independencia del poder Ejecutivo y los poderes de investigación y sanción de las autoridades para la protección de datos personales en cada Estado.
6. Impulsar y fortalecer el trabajo de la Red Iberoamericana de Protección de Datos como foro en el que se encuentran las autoridades de protección de datos de la región.
7. Ajustar las legislaciones nacionales para que regulen la protección de datos de forma convergente, a partir de estándares mínimos de protección. Esto con el fin de que las empresas transnacionales puedan adaptarse al mercado de los cuatro países, sin el riesgo de la fragmentación y, además, de aumentar el poder de negociación de los países de la región frente a las EMNBD transnacionales. Una forma adecuada y viable de realizar lo anterior es avanzar a partir de los acuerdos mínimos alcanzados en los Estándares de protección de datos para los Estados iberoamericanos creados por la Red Iberoamericana de Protección de Datos.
8. A partir de los mínimos anteriores, debidamente incorporados en las legislaciones locales, impulsar la creación de una regulación regional común a los Estados latinoamericanos, ajustada a las dinámicas de la era digital. Una regulación que permita, a la vez, la promesa de la eficacia del derecho fundamental a la protección de datos personales de los nacionales de estos Estados y hacerle frente, como región, al poder de las EMNBD transnacionales.

Referencias

Asamblea General de las Naciones Unidas (ONU). Declaración Universal de Derechos Humanos. París, 1948. Consultado marzo 24, 2020. https://www.un.org/es/universal-declaration-human-rights/

Büchi, Moritz, Eduard Fosch-Villaronga, Chirstoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi y Salome Viljoen. "Chilling Effects of Profiling Activities: Mapping the Issues". SSRN, 2019. Consultado enero 8, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3379275

Constitución Política de Colombia [Const]. Julio 7 de 1991 (Colombia). http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

Constitución Política de la República Federativa de Brasil [Const]. Octubre 5, 1988 (Brasil). https://www.acnur.org/fileadmin/Documentos/BDL/2001/0507.pdf

Constitución Política de los Estados Unidos Mexicanos [Const]. Febrero 05, 1917 (Estados Unidos Mexicanos). https://www.juridicas.unam.mx/legislacion/ordenamiento/constitucion-politica-de-los-estados-unidos-mexicanos

Convenio 108 de 1981 [Consejo de Europa]. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Enero 28, 1981. https://rm.coe.int/16806c1abd

Directiva 95/46 de 1995 [Parlamento Europeo y Consejo Europeo]. Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Octubre 24, 1995. Consulado marzo 24, 2020. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Estados Unidos Mexicanos. Secretaría de Gobernación. 2Lineamientos del Aviso de Privacidad". 17 de enero de 2013. http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

Gräf, Eike. "When Automated Profiling Threatens Our Freedom: A Neo-Republican Perspective". European Data Protection Law Review, 3(4) 2017, 441-451.

Kandias, Miltiadis, Lilian Mitrou, Vasilis Stavrou y Dimistris Gritzalis. "Profiling Online Social Networks users: An Omniopticon tool". International Journal of Social Networks Mining, 2(4) 2016: 293-313.

Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 18 de 2012. D.O. 48.587. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Marder, Ben, Adam Joinson, Avi Shankar y David Houghton. "The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking". Computers in Human Behavior, 60 (2016), 582-592.

Naciones Unidas (ONU). Pacto Internacional de Derechos Civiles y Políticos. New York, 1966. Consultado marzo 24, 2020. https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Naciones Unidas (ONU). *Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar"*. Nueva York y Ginebra: ONU, 2011. Consultado marzo 24, 2020. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_sp.pdf

Observación General No. 16 de 1988 [Comité de los Derechos Humanos]. Comentarios generales adoptados por el Comité de los Derechos Humanos, Artículo 17. 1988. http://hrlibrary.umn.edu/hrcommittee/Sgencom16.html

Organización de los Estados Americanos, Consejo Presidencial Andino. *Declaración de Santa Cruz de La Sierra*. Enero 30, 2003. Consultado marzo 24, 2020. https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf

Red Iberoamericana de Protección de Datos. Estándares de protección de datos personales para los Estados Iberoamericanos. Junio 20. 2017. Consultado marzo 24. 2020. https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ce (Reglamento general de protección de datos -GDPR-) 27 de abril de 2016. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Resolución A/C.3/71/L.39 [Asamblea General de las Naciones Unidas]. El derecho a la privacidad en la era digital. Octubre 31, 2016. Consultado marzo 24. 2020. https://documents-dds-ny.un.org/doc/UNDOC/LTD/N16/388/46/PDF/N1638846.pdf?OpenElement

Resolución A/HRC/RES/17/4 [Asamblea General de las Naciones Unidas]. Los derechos humanos y las empresas transnacionales y otras empresas. Julio 6, 2011. https://undocs.org/en/A/HRC/RES/17/4

Unión Europea. Carta de los Derechos Fundamentales de la Unión Europea. Diario Oficial de las Comunidades Europeas. C 364/1. Diciembre 18, 2000. Consultado marzo 24, 2020. https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Biografías de los autores

Kimberly Anastácio: Licenciada y Magíster en Ciencia Política, Universidad de Brasilia. Fue investigadora en el Departamento de Políticas Públicas, Fundação Getulio Vargas y es coordinadora de datos, Isobar. Colabora con Coding Rights en temas de derechos humanos e internet.

María Paula Ángel Arango: Abogada *cum laude* y politóloga, Universidad de los Andes, Magíster en Derecho Administrativo, Universidad del Rosario. En 2019 recibió la beca Fullbright-Colciencias para estudios de doctorado. Actualmente es estudiante de doctorado en Derecho en la Universidad de Washington, Seattle, y asistente de investigación del UW Tech Policy Lab.

Paloma Herrera Carpintero: Abogada. Licenciada en Ciencias Jurídicas y Sociales, Universidad de Chile. Diplomado en Ciberseguridad, Universidad de Chile. Colaboradora en el Centro de Estudios en Derecho Informático, Universidad de Chile.

Vivian Newman Pont: Abogada, Universidad Javeriana y licenciada en derecho por homologación, Universidad de Barcelona, con posgrado en derecho administrativo (D.S.U.) y maestría (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, Universidad de los Andes e investigador de Dejusticia.

Bruna Santos: Abogada, Centro Universitário de Brasilia y analista de Coding Rights. Co-coordinadora de Internet Governance Caucus y miembro de Non-Commercial Users Constituency en la Corporação da Internet para Atribuição de Nomes e Números.

Milan Trnka Osorio: Abogado, Universidad Nacional Autónoma de México (UNAM). Oficial jurídico en R3D: Red en Defensa de los Derechos Digitales.

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

Joana Varon: Directora ejecutiva de Coding Rights, fellow de Mozilla Foundation, afiliada al Berkman Klein Center for Internet and Society de la Universidad de Harvard, miembro del Consejo Consultivo de Open Technology Fund.

Pablo Viollier Bonvin: Abogado. Licenciado en Ciencias Jurídicas y Sociales y diplomado en ciberseguridad, Universidad de Chile. Actualmente se desempeña como analista de políticas públicas de Derechos Digitales y docente, Universidad Diego Portales.

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 1

ETNORREPARACIONES: la justicia colectiva étnica y la reparación a pueblos indígenas y comunidades afrodescendientes en Colombia

Publicación digital e impresa

César Rodríguez Garavito, Yukyan Lam

2011

• DOCUMENTOS 2

LA CONSULTA PREVIA: DILEMAS Y SOLUCIONES. Lecciones del proceso de construcción del decreto de reparación y restitución de tierras para pueblos indígenas en Colombia

Publicación digital e impresa

César Rodríguez Garavito, Natalia Orduz Salinas

2012

• DOCUMENTOS 3

LA ADICCIÓN PUNITIVA: La desproporción de leyes de drogas en América Latina

Publicación digital e impresa

Rodrigo Uprimny, Diana Esther Guzmán, Jorge Parra Norato

2012

• DOCUMENTOS 4

ORDEN PÚBLICO Y PERFILES RACIALES: experiencias de afrocolombianos con la policía en Cali

Publicación digital e impresa

Yukyan Lam, Camilo Ávila

2013

• DOCUMENTOS 5

INSTITUCIONES Y NARCOTRÁFICO: la geografía judicial de los delitos de drogas en Colombia

Publicación digital

Mauricio García Villegas, Jose Rafael Espinosa Restrepo, Felipe Jiménez Ángel

2013

• DOCUMENTOS 6

ENTRE ESTEREOTIPOS: Trayectorias laborales de mujeres y hombres en Colombia

Publicación digital

Diana Esther Guzmán, Annika Dalén

2013

• DOCUMENTOS 7

LA DISCRIMINACIÓN RACIAL EN EL TRABAJO: Un estudio experimental en Bogotá

Publicación digital e impresa

César Rodríguez Garavito, Juan Camilo Cárdenas C., Juan David Oviedo M., Sebastián Villamizar S.

2013

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 8

LA REGULACIÓN DE LA INTERRUPCIÓN VOLUNTARIA DEL EMBARAZO EN COLOMBIA

Publicación digital

Annika Dalén, Diana Esther Guzmán, Paola Molano

2013

• DOCUMENTOS 9

ACOSO LABORAL

Publicación digital

Diana Guzmán, Annika Dalén

2013

• DOCUMENTOS 10

ACCESO A LA JUSTICIA: Mujeres, conflicto armado y justicia

Publicación digital

Diana Esther Guzmán Rodríguez, Sylvia Prieto Dávila

2013

• DOCUMENTOS 11

LA IMPLEMENTACIÓN DE LA DESPENALIZACIÓN PARCIAL DEL ABORTO

Publicación digital e impresa

Annika Dalén

2013

• DOCUMENTOS 12

RESTITUCIÓN DE TIERRAS Y ENFOQUE DE GÉNERO

Publicación digital e impresa

Diana Esther Guzmán, Nina Chaparro

2013

• DOCUMENTOS 13

RAZA Y VIVIENDA EN COLOMBIA: la segregación residencial y las condiciones de vida en las ciudades

Publicación digital e impresa

María José Álvarez Rivadulla, César Rodríguez Garavito, Sebastián Villamizar Santamaría, Natalia Duarte

2013

• DOCUMENTOS 14

PARTICIPACIÓN POLÍTICA DE LAS MUJERES Y PARTIDOS. Posibilidades a partir de la reforma política de 2011.

Publicación digital

Diana Esther Guzmán Rodríguez, Sylvia Prieto Dávila

2013

• DOCUMENTOS 15

BANCADA DE MUJERES DEL CONGRESO: una historia por contar

Publicación digital

Sylvia Cristina Prieto Dávila, Diana Guzmán Rodríguez

2013

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 16

OBLIGACIONES CRUZADAS: Políticas de drogas y derechos humanos

Publicación digital

Diana Guzmán, Jorge Parra, Rodrigo Uprimny

2013

• DOCUMENTOS 17

GUÍA PARA IMPLEMENTAR DECISIONES SOBRE DERECHOS SOCIALES
Estrategias para los jueces, funcionarios y activistas

Publicación digital e impresa

César Rodríguez Garavito, Celeste Kauffman

2014

• DOCUMENTOS 18

VIGILANCIA DE LAS COMUNICACIONES EN COLOMBIA
El abismo entre la capacidad tecnológica y los controles legales

Publicación digital e impresa

Carlos Cortés Castillo

2014

• DOCUMENTOS 19

NO INTERRUMPIR EL DERECHO
Facultades de la Superintendencia Nacional de Salud en materia de IVE

Publicación digital

Nina Chaparro González, Annika Dalén

2015

• DOCUMENTOS 20

DATOS PERSONALES EN INFORMACIÓN PÚBLICA: oscuridad en lo privado y luz en lo público

Publicación digital e impresa

Vivian Newman

2015

• DOCUMENTOS 21

REQUISAS, ¿A DISCRECIÓN?
Una tensión entre seguridad e intimidad

Publicación digital e impresa

Sebastián Lalinde Ordóñez

2015

• DOCUMENTOS 22

FORMACIÓN EN VIOLENCIA SEXUAL EN EL CONFLICTO ARMADO: una propuesta metodológica para funcionarios

Publicación digital

Silvia Rojas Castro, Annika Dalén

2015

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 23

CASAS DE JUSTICIA:
una buena idea mal administrada

Publicación digital

Equipo de investigación: Mauricio García Villegas,
Jose Rafael Espinosa Restrepo, Sebastián Lalinde Ordóñez,
Lina Arroyave Velásquez, Carolina Villadiego Burbano
2015

• DOCUMENTOS 24

LOS REMEDIOS QUE DA EL DERECHO.
El papel del juez constitucional cuando la interrupción
del embarazo no se garantiza

Publicación digital

Diana Esther Guzmán, Nina Chaparro González
2015

• DOCUMENTOS 25

EL EJERCICIO DE LA INTERRUPCIÓN VOLUNTARIA
DEL EMBARAZO EN EL MARCO DEL CONFLICTO ARMADO

Publicación digital

Margarita Martínez Osorio, Annika Dalén,
Diana Esther Guzmán, Nina Chaparro González
2015

• DOCUMENTOS 26

CUIDADOS PALIATIVOS:
abordaje de la atención en salud
desde un enfoque de derechos humanos

Publicación digital e impresa

Isabel Pereira Arana
2016

• DOCUMENTOS 27

SARAYAKU ANTE EL SISTEMA INTERAMERICANO
DE DERECHOS HUMANOS:
justicia para el pueblo del Medio Día y su selva viviente

Publicación digital e impresa

Mario Melo Cevallos
2016

• DOCUMENTOS 28 IDEAS PARA CONSTRUIR LA PAZ

LOS TERRITORIOS DE LA PAZ.
La construcción del estado local en Colombia

Publicación digital e impresa

Mauricio García Villegas, Nicolás Torres Echeverry,
Javier Revelo Rebolledo, Jose R. Espinosa Restrepo,
Natalia Duarte Mayorga
2016

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 29 IDEAS PARA CONSTRUIR LA PAZ

NEGOCIANDO DESDE LOS MÁRGENES:
la participación política de las mujeres en los procesos de paz en Colombia (1982-2016)

Publicación digital e impresa

Nina Chaparro González, Margarita Martínez Osorio
2016

• DOCUMENTOS 30 IDEAS PARA CONSTRUIR LA PAZ

LA PAZ AMBIENTAL:
retos y propuestas para el posacuerdo

Publicación digital e impresa

César Rodríguez Garavito, Diana Rodríguez Franco, Helena Durán Crane
2016

• DOCUMENTOS 31 IDEAS PARA CONSTRUIR LA PAZ

ACCESO A LOS ARCHIVOS DE INTELIGENCIA Y CONTRAINTELIGENCIA EN EL MARCO DEL POSACUERDO

Publicación digital e impresa

Ana María Ramírez Mourraille, María Paula Ángel Arango, Mauricio Albarracín Caballero, Rodrigo Uprimny Yepes, Vivian Newman Pont
2017

• DOCUMENTOS 32

JUSTICIA TRANSICIONAL Y ACCIÓN SIN DAÑO
Una reflexión desde el proceso de restitución de tierras

Publicación digital e impresa

Aura Patricia Bolivar Jaime, Olga del Pilar Vásquez Cruz
2017

• DOCUMENTOS 33

SIN REGLAS NI CONTROLES
Regulación de la publicidad de alimentos y bebidas dirigida a menores de edad

Publicación digital e impresa

Diana Guarnizo Peralta
2017

• DOCUMENTOS 34

ACADEMIA Y CIUDADANÍA
Profesores universitarios cumpliendo y violando normas

Publicación digital e impresa

Mauricio García Villegas, Nicolás Torres Echeverry, Andrea Ramírez Pisco, Juan Camilo Cárdenas Campo
2017

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 35 IDEAS PARA CONSTRUIR LA PAZ

ESTRATEGIAS PARA UNA REFORMA RURAL TRANSICIONAL

Publicación digital e impresa

Nelson Camilo Sánchez León

2017

• DOCUMENTOS 36 IDEAS PARA CONSTRUIR LA PAZ

SISTEMA DE JUSTICIA TERRITORIAL PARA LA PAZ

Publicación digital e impresa

Carolina Villadiego Burbano, Sebastián Lalinde Ordóñez

2017

• DOCUMENTOS 37

DELITOS DE DROGAS Y SOBREDOSIS CARCELARIA EN COLOMBIA

Publicación digital e impresa

Rodrigo Uprimny Yepes, Sergio Chaparro Hernández, Luis Felipe Cruz Olivera

2017

• DOCUMENTOS 38 IDEAS PARA CONSTRUIR LA PAZ

COCA, INSTITUCIONES Y DESARROLLO

Los retos de los municipios productores en el posacuerdo

Publicación digital e impresa

Sergio Chaparro Hernández, Luis Felipe Cruz Olivera

2017

• DOCUMENTOS 39 IDEAS PARA CONSTRUIR LA PAZ

RESTITUCIÓN DE TIERRAS, POLÍTICA DE VIVIENDA Y PROYECTOS PRODUCTIVOS

Ideas para el posacuerdo

Publicación digital e impresa

Aura Patricia Bolivar Jaime, Angie Paola Botero Giraldo, Laura Gabriela Gutiérrez Baquero

2017

• DOCUMENTOS 40

CÁRCEL O MUERTE

El secreto profesional como garantía fundamental en casos de aborto

Publicación digital

Ana Jimena Bautista Revelo, Anna Joseph, Margarita Martínez Osorio

2017

• DOCUMENTOS 41

SOBREDOSIS CARCELARIA Y POLÍTICA DE DROGAS EN AMÉRICA LATINA

Publicación digital e impresa

Sergio Chaparro Hernández, Catalina Pérez Correa

2017

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 42

SOBREPESO Y CONTRAPESOS
La autorregulación de la industria no es suficiente para proteger a los menores de edad

Publicación digital e impresa

Valentina Rozo Rangel

2017

• DOCUMENTOS 43

VÍCTIMAS Y PRENSA DESPUÉS DE LA GUERRA
Tensiones entre intimidad, verdad histórica y libertad de expresión

Publicación digital e impresa

Vivian Newman Pont, María Paula Ángel Arango, María Ximena Dávila Contreras

2018

• DOCUMENTOS 44

LO QUE NO DEBE SER CONTADO
Tensiones entre el derecho a la intimidad y el acceso a la información en casos de interrupción voluntaria del embarazo

Publicación digital

Nina Chaparro González, Diana Esther Guzmán, Silvia Rojas Castro

2018

• DOCUMENTOS 45

POSCONFLICTO Y VIOLENCIA SEXUAL
La garantía de la interrupción voluntaria del embarazo en los municipios priorizados para la paz

Publicación digital

Ana Jimena Bautista Revelo, Blanca Capacho Niño, Margarita Martínez Osorio

2018

• DOCUMENTOS 46

UN CAMINO TRUNCADO: LOS DERECHOS SEXUALES Y REPRODUCTIVOS EN MONTES DE MARÍA

Publicación digital e impresa

María Ximena Dávila, Margarita Martínez, Nina Chaparro

2019

• DOCUMENTOS 47

ETIQUETAS SIN DERECHOS. Etiquetado de productos comestibles: un análisis desde los derechos humanos

Publicación digital e impresa

Diana Guarnizo, Ana María Narváez

2019

COLECCIÓN DOCUMENTOS DEJUSTICIA

• DOCUMENTOS 48

RENDICIÓN DE CUENTAS DE GOOGLE Y OTROS NEGOCIOS EN COLOMBIA: la protección de datos personales en la era digital

Publicación digital e impresa

Vivian Newman Pont, María Paula Ángel Arango

2019

• DOCUMENTOS 49

ELOGIO A LA BULLA: protesta y democracia en Colombia

Publicación digital e impresa

Sebastián Lalinde Ordóñez

2019

• DOCUMENTOS 50

LOS TERCEROS COMPLEJOS: la competencia limitada de la Jurisdicción Especial para la Paz

Publicación digital e impresa

Sabine Michalowski, Alejandro Jiménez Ospina, Hobeth Martínez Carrillo, Daniel Marín López

2019

• DOCUMENTOS 51

DIME DÓNDE ESTUDIAS Y TE DIRÉ QUÉ COMES
Oferta y publicidad en tiendas escolares de Bogotá

Publicación digital e impresa

Valentina Rozo Ángel

2019

• DOCUMENTOS 52

LOS CAMINOS DE DOLOR
Acceso a cuidados paliativos y tratamiento por consumo de heroína en Colombia

Publicación digital e impresa

Isabel Pereira, Lucía Ramírez

2019

• DOCUMENTOS 53

LOS SEGUNDOS OCUPANTES EN EL PROCESO DE RESTITUCIÓN DE TIERRAS:
RETO A LA REPARACIÓN CON VOCACIÓN TRANSFORMADORA

Publicación digital e impresa

Hobeth Martínez Carrillo

2019

• Documentos 54

CANNABIS EN LATINOAMÉRICA: LA OLA VERDE Y LOS RETOS HACIA LA REGULACIÓN

Publicación digital e impresa

Alejandro Corda, Ernesto Cortés, Diego Piñol Arriagada

2019

COLECCIÓN **DOCUMENTOS** DEJUSTICIA

• Documentos 55

ACCESO, PROMOCIÓN Y PERMANENCIA DE NIÑOS, NIÑAS Y ADOLESCENTES MIGRANTES EN EL SISTEMA EDUCATIVO COLOMBIANO. AVANCES, RETOS Y RECOMENDACIONES

Publicación digital e impresa

Silvia Ruiz Mancera, Lucía Ramírez Bolívar, Valentina Rozo Ángel

2020

• Documentos 56

ENTRE LA BATA Y LA TOGA: EL ROL DE LOS TRIBUNALES DE ÉTICA MÉDICA EN LA GARANTÍA DE LOS DERECHOS SEXUALES Y REPRODUCTIVOS

Publicación digital e impresa

María Ximena Dávila, Nina Chaparro

2020

• Documentos 57

LA IMAGINACIÓN MORAL EN EL TRÁNSITO HACIA LA PAZ

Publicación digital

Ivonne Elena Díaz García

2020

DOCUMENTOS 58

En conversación con Mark Zuckerberg, Yuval Noah Harari (historiador y filósofo israelí) se pregunta por los peligros de los sistemas computarizados que nos conocen mejor que nuestra propia madre, sistemas cuyos intereses no están necesariamente alineados con los intereses de las personas.
La acumulación de información a gran escala, afirma, supone la emergencia de un tipo de poder sin precedentes en la historia de la humanidad. Este libro es un intento por abordar los múltiples desafíos de este nuevo tipo de poderosos sistemas. Pretende mostrar cómo las empresas en la era digital realizan recolección masiva de datos personales y cómo están lidiando con el poder que otorga la acumulación de información, mientras intentan avanzar su estrategia de negocios y, en el caso de los gigantes de Internet —Google, Amazon, Facebook, Apple y Microsoft—, remodelar el comportamiento de individuos y ciudadanos por fuera de las fronteras territoriales de los Estados-Nación. El libro analiza las políticas de privacidad de algunas empresas con modelos de negocios basados en datos en cuatro países de América Latina: Brasil, Chile, Colombia y México. Asimismo, evalúa qué tan preparados se encuentran estos Estados para proteger a sus ciudadanos de la explotación masiva de datos personales y para hacerles frente a los desafíos legales del tratamiento automatizado de grandes cantidades de datos en un contexto trasnacional, en constante transformación y con actores tan o más poderosos que los propios Estados-Nación.