Rendición de cuentas de Google y otros negocios en Colombia:

la protección de datos personales en la era digital

Vivian Newman Pont
María Paula Ángel Arango

DOCUMENTOS 48

Dejusticia
derecho · justicia · sociedad

DOCUMENTOS 48

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.) 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 subdirectora de Dejusticia. Sus últimas publicaciones incluyen: *Datos personales en información pública: oscuridad en lo privado y luz en lo público* (2015) y en coautoría *Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo* (2017), *Sobre la corrupción en Colombia: marco conceptual, diagnóstico y propuestas de política* (2017) y *Víctimas y prensa después de la guerra. Tensiones entre intimidad, verdad histórica y libertad de expresión* (2018).

María Paula Ángel Arango Abogada Cum Laude y politóloga de la Universidad de los Andes. Estudiante de la maestría en Derecho Administrativo de la Universidad del Rosario. Actualmente se desempeña como investigadora en la sublínea de Transparencia e Intimidad en Dejusticia. Sus últimas publicaciones incluyen, en coautoría: *Acceso a los archivos de inteligencia y contrainteligencia en el marco del posacuerdo* (2017), *Sobre la corrupción en Colombia: marco conceptual, diagnóstico y propuestas de política* (2017) y *Víctimas y prensa después de la guerra. Tensiones entre intimidad, verdad histórica y libertad de expresión* (2018).

Rendición de cuentas de Google y otros negocios en Colombia:

la protección de datos personales en la era digital

Vivian Newman Pont

María Paula Ángel Arango

Dejusticia
derecho · justicia · sociedad

Documentos Dejusticia 48
RENDICIÓN DE CUENTAS DE GOOGLE Y OTROS NEGOCIOS EN COLOMBIA:
la protección de datos personales en la era digital

ISBN: 978-958-5441-66-8 Versión digital
978-958-5441-66-8 Versión impresa

Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia
Carrera 24 Nº 34-61, Bogotá, D.C.
Teléfono: (57 1) 608 3605
Correo electrónico: info@dejusticia.org
https://www.dejusticia.org

Revisión de textos: María José Díaz Granados
Preprensa: Marta Rojas
Cubierta: Alejandro Ospina

Bogotá, enero de 2019

Contenido

Agradecimientos

Nuestra investigación no hubiera sido posible sin el apoyo temático y financiero de la organización Privacy International, a la que expresamos nuestro gratitud. Además, la ayuda y el acompañamiento que recibimos de Alexandrine Pirlot de Corbion, Francisco Vera y en especial de Ailidh Callander fueron fundamentales para el enriquecimiento del contenido de este documento. Así mismo, la retroalimentación de Juan Carlos Upegui contribuyó en gran medida al desarrollo exitoso de este proceso.

Agradecemos también a nuestros amigos y colegas de Dejusticia, que asistieron al seminario de discusión realizado y se tomaron el tiempo de leer y comentar el primer borrador de este texto. También quisiéramos agradecer a Carlos Cortés, José Alejandro Bermúdez, Daniel Castaño, Viviana Cañon, Juan Diego Castañeda, Grenfieth J. Sierra, Camilo de la Cruz, Lorena Lizarazo, Ana Carolina Molina, Celso Bessa y Gabriela Hadid, que generosamente asistieron a nuestro grupo focal y enriquecieron el contenido de este documento con sus experiencias y puntos de vista. Muchas gracias también a Laura Guerrero y a Sophie Kushen, quienes aportaron de manera sustancial en los cambios finales del texto.

Por último, gracias al equipo administrativo de Dejusticia por su colaboración constante en la realización de las labores diarias. Particularmente, agradecemos a Elvia Sáenz y a Isabel De Brigard por su ayuda e infaltable buena disposición en el proceso editorial de este documento.

Introducción

Hoy en día es recurrente oír que los datos son el nuevo petróleo.[1] ¿De qué datos estamos hablando? Hablamos de los datos digitales que son constantemente recolectados o generados por las tecnologías de la información y la comunicación (TIC), como el internet, las redes sociales, nuestros dispositivos móviles, las aplicaciones que tenemos en ellos, nuestra tarjeta inteligente de transporte público, o los sensores del motor de nuestro carro o de nuestros relojes inteligentes, por citar solo algunos ejemplos. Y ¿en qué se basan quienes pronuncian esa afirmación con tanta seguridad? En que si son adecuadamente refinados y explotados, los datos digitales –al igual que el petróleo o cualquier unidad de medida con alto valor– pueden generar valor económico y social para los países y para las empresas.[2] ¿Cómo? Al revelar patrones, correlaciones y otra información y conocimiento que, sin los datos y la analítica de datos, sería imposible develar.

En consecuencia, alrededor del mundo se han creado miles de empresas que buscan capturar ese valor. Entre ellas, sobresalen por su tamaño y poder económico, tecnológico y social Google, Apple, Facebook, Amazon y Microsoft (en adelante Gafam), pero también empresas intermedias

1 Si bien el origen de esta afirmación es atribuido a Clive Humby, matemático inglés y creador de la Clubcard de Tesco, la misma ha sido repetida por varios "capitalistas de la tecnología". Al respecto, ver Michael Haupt (2016).

2 Según el McKinsey Global Institute, "hay *fuerte* evidencia de que el Big Data puede jugar un rol económico significativo para beneficio no solo del comercio privado sino también de las economías nacionales y de sus ciudadanos. Nuestra investigación encuentra que los datos pueden crear un valor significativo para la economía mundial, mejorando la productividad y competitividad de las compañías y del sector público, y creando un excedente económico sustancial para los consumidores" (Manyika, Chui, Brown, Bughin, Dobbs y Roxburgh *et al.*, 2011, pp. 1-2).

y múltiples *start-ups* digitales. Del mismo modo, varias empresas ya establecidas también han empezado a extraer el valor de los datos con los que cuentan, para optimizar procesos, mejorar sus estrategias de mercadeo, o la calidad y funcionalidad de los bienes y servicios que ofrecen. Esa colección de empresas, que en conjunto denominaremos "empresas con modelos de negocio basados en datos" (en adelante EMNBD),[3] están revolucionando la economía y la han llevado a lo que hoy conocemos como la economía digital, lo que a su vez termina por afectar la política y los derechos de la ciudadanía.

La economía digital tiene su piedra angular en el *big data* (Corredor, 2015, pp. 1-26), 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, p. 8). Si bien es cierto que no todo el *big data* corresponde a datos personales, lo cierto es que "gran parte de la información que ahora se genera incluye información personal. Y las empresas tienen una gran cantidad de incentivos para capturar más, mantenerlo más tiempo y reutilizarlo a menudo" (Mayer-Schönberger y Cukier, 2013, p. 152). Además, como consecuencia de los grandes volúmenes de datos que se están generando hoy en día y de los avances tecnológicos para procesar dichos datos (los llamados "data analytics" o "procesos de Big Data"), el concepto de dato personal parece haberse ampliado. Así, ahora "la PII [información de identificación personal] también se trata de la cantidad de datos; cuanta más información tenga alguien sobre usted, incluso información anónima, más fácil le resultará identificarlo" (Schneir, 2015, p. 53).

---

3 Si bien ese concepto hace referencia, en general, a las empresas con "modelos de negocio que confían en los datos *como un recurso clave*" (Hartmann, Zaki, Feldmann y Hartmann, 2014, p. 6) (énfasis agregado), existen varios modelos de negocio basados en datos. Es decir, varias formas en las que, por medio del uso y la explotación de datos, "la[s] empresa[s] gana[n] dinero y sustenta[n] los flujos de ingresos a lo largo del tiempo" (Alcaíno, Arenas y Gutiérrez, 2015, p. 12). En particular, existen seis dimensiones a través de las cuales se pueden clasificar las EMNBD, a saber: i) recursos clave (fuente de datos), ii) actividades clave, iii) propuesta de valor, iv) segmento de clientes al que se dirige, v) modelo de ingresos y, vi) estructura de costos (Hartmann *et al.*, 2014; Alcaíno *et al.*, 2015). Así, a partir de esas seis dimensiones, en el Anexo 2 de este documento se exponen las distintas clases de modelos de negocio basados en datos que pueden existir.

Por eso, el desarrollo de la economía digital y del *big data* plantea desafíos importantes para los derechos a la intimidad[4] y a la protección de datos personales[5] de las personas, así como para la transparencia, la seguridad de los datos y el derecho a la igualdad. Al respecto, en la Unión Europea el Grupo de Trabajo del Artículo 29[6] ha dicho que en el marco de la protección de los datos personales el *big data* genera preocupaciones sobre los siguientes cuatro temas:[7] i) "la gran escala de recopilación de datos, seguimiento y elaboración de perfiles, teniendo también en cuenta la variedad y el detalle de los datos recopilados y el hecho de que los datos se combinan a menudo de muchas fuentes diferentes";[8] ii) "la seguridad de los datos, con niveles de protección que se quedan atrás de su expansión en volumen";[9] iii) la "transparencia: a menos que se les proporcione información suficiente, las personas estarán sujetas a decisiones que no comprenden y de las cuales no tienen control";[10] y, iv) "inexactitud,

4 Entendido aquí como el derecho humano que protege a las personas contra atentados que afectan tanto el secreto de su vida privada, como la libertad que en ella se ejerce. Al respecto, ver Corte Constitucional, Sentencia T-222 de 1992, M. P. Ciro Angarita Barón.

5 Entendido aquí como el derecho humano "que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales". Ver Corte Constitucional, Sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett.

6 El Grupo de Trabajo fue establecido por el Artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, como el organismo consultivo independiente de la Unión Europea en materia de protección de datos y privacidad. Está conformado por el supervisor europeo de protección de datos, la Comisión Europea y por un representante de la Autoridad de Protección de Datos de cada Estado miembro de la Unión Europea. A partir de la entrada en vigencia del Reglamento General de Protección de Datos (25 de mayo de 2018), el Grupo de Trabajo del Artículo 29 se ha convertido en el Comité Europeo de Protección de Datos.

7 El Grupo de Trabajo identificó también como preocupación las mayores posibilidades de vigilancia por parte del Gobierno. Sin embargo, dado que en este documento nos concentramos en las prácticas que adelantan las empresas privadas con base en los datos, preferimos dejarlo por fuera de la enumeración de riesgos, para no distraer la atención del lector.

8 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.

9 *Idem.*

10 *Idem.*

discriminación, exclusión y desequilibrio económico".[11] En resumen, lo que le preocupa al Grupo de Trabajo es que la disponibilidad de grandes volúmenes de datos digitales y las capacidades actuales para encontrar correlaciones entre los datos puedan hacer que se deriven o infieran otros datos personales o se creen perfiles de los titulares de los datos, que puedan ser tanto exactos como inexactos,[12] a partir de los cuales se puedan tomar decisiones –a veces injustas o discriminatorias– sobre dichos titulares, sin que ellos mismos tengan seguridad, conocimiento ni control de lo que sucede a partir de sus datos.

Ejemplos de los riesgos que el *big data* plantea para los derechos a la intimidad y a la protección de datos personales pueden tomarse del sonado caso de la cadena de almacenes Target, cuya analítica de datos le permitió inferir, a partir de los datos de compras de sus clientes, el embarazo de una cliente adolescente, incluso antes de que sus padres lo supieran (Forbes, 2012). Por su parte, los riesgos para la transparencia y para la seguridad de los datos son evidentes en el escándalo de Facebook y Cambridge Analytica, en el que Facebook permitió el uso de una aplicación que terminó recolectando información de 87 millones de perfiles de usuarios de todo el mundo, que luego sería utilizada por Cambridge Analytica para influenciar electores en la campaña presidencial de Estados Unidos en 2016, y en el referendo sobre la permanencia del Reino Unido en la Unión Europea. Frente a este último caso, la Oficina del Comisionado de Información (ICO) del Reino Unido finalmente concluyó que Facebook no salvaguardó adecuadamente la información de sus usuarios y que no fue transparente sobre la forma en la que otros recopilarían esa información (*The Guardian*, 2018). Finalmente, ejemplos de discriminación producida a través del uso del *big data* pueden extraerse de la investigación adelantada por la Universidad de Washington en 2015, en la que se encontró que al buscar la palabra "C.E.O." en el buscador de imágenes de Google, los resultados arrojados corresponden en tan solo un 11% a mujeres, a pesar de que el 27% de los jefes ejecutivos en Estados Unidos son mujeres (Kay, Matuszek y Munson, 2015, pp. 1-10). Del mismo modo, una investigación de la Universidad Carnegie Mellon publicada en 2015 encontró que el sistema de publicidad en línea de Google le muestra con mayor

11 *Idem.*

12 Según Frederike Kaltheuner, la vigilancia que funciona nos lleva a un mundo orwelliano (*Orwellian*), mientras que la que es inexacta nos transporta a un mundo kafkiano (*Kafkaesque*) (Joanne McNeil, s. f.).

frecuencia a los hombres, en comparación con las mujeres, los anuncios de empleos de altos ingresos (Datta, Tschantz y Datta, 2015, pp. 92-112).

De hecho, fue precisamente en respuesta a ese tipo de riesgos que el Parlamento Europeo y el Consejo de la Unión Europea expidieron el Reglamento General de Protección de Datos (Reglamento [UE] 2016/679) (GDPR, por sus siglas en inglés), el cual entró finalmente en vigencia el 25 de mayo de 2018 y pretendió actualizar la legislación de protección de datos personales en la Unión Europea. Entre sus finalidades se destaca intentar equilibrar la protección de los derechos a la intimidad y a la protección de datos personales con el desarrollo económico y la innovación. Por eso, el supervisor europeo de protección de datos, Giovanni Buttarelli, describió el GDPR como "una actualización radical del libro de reglas para la era digital" (Irish Tech News, 2018).

Del mismo modo, y a pesar de la inexistencia de una ley integral de protección de datos que se aplique en todo Estados Unidos,[13] en el estado de California recientemente se promulgó la Ley de Privacidad del Consumidor de California, A.B. 375 (CCPA, por sus siglas en inglés), que entrará en vigencia en enero de 2020. Al igual que el GDPR, en cuyas disposiciones se inspiró, el CCPA de California pretende dar al usuario un mayor control sobre la forma en la que las empresas recopilan y usan su información personal. Así, si bien no resuelve todos los problemas que enfrenta hoy en día el derecho a la privacidad, el CCPA es "un muy buen siguiente paso mientras trabajamos para empoderar a los ciudadanos y proteger a la misma democracia de la recopilación de datos salida de control" (McDonald, 2018, p. 4). Además, el impacto de esta nueva ley se ve potenciado por el peso que tiene California en Estados Unidos, pues su población y el gran tamaño de su economía otorgan a sus leyes una influencia considerable en el resto del país. De esta manera, por razones de coherencia y eficiencia, las empresas pueden optar por cumplir con las leyes de California incluso en otros estados. Además, muchas de las grandes

13 Al respecto, es importante notar que si bien no existe una única ley federal de protección de datos, a partir de marzo de 2018 (y en parte a raíz de los múltiples escándalos de violación de datos como el de Cambridge Analytica), todos los estados, así como el Distrito de Columbia, Guam, Puerto Rico y las Islas Vírgenes de los Estados Unidos han implementado leyes de notificación de incumplimiento, que requieren que las compañías notifiquen a los usuarios si se abusa de sus datos personales (Serrato, Cwalina, Rudawski, Coughlin y Fardelmann, 2018).

empresas de internet tienen su sede en California, lo que hace que este paso sea aún más significativo.

Pero ¿cómo ha enfrentado la región latinoamericana estos mismos retos? A diferencia de la Unión Europea, en América Latina aún "no parece haber surgido un enfoque 'regional' uniforme y coherente"[14] al respecto. Lo anterior, a pesar de que entre 2013 y 2018 el número de usuarios de internet en Latinoamérica creció de 278,1 millones a 375,1 millones, y se proyecta que para 2019 alcance los 387,2 millones de usuarios (Statista, 2018a). Además, y en lo que respecta a los Gafam, a agosto de 2017 Google tenía una participación de más del 90% del mercado de motores de búsqueda en México, Venezuela, Argentina, Brasil, Bolivia, Colombia, Chile y Perú (Statista, 2018b). Por su parte, entre 2014 y 2018 el número de usuarios de Facebook en Latinoamérica creció de 194,1 millones a 271,1 millones, y se espera que alcance los 282,2 millones para 2019 (Statista, 2018c). Asimismo, entre 2014 y 2018 en América Latina el número de compradores de bienes y servicios en línea pasó de 103,9 millones a 147,2 millones, y se estima que para 2019 ese número alcanzará los 155,5 millones de compradores *online* (Statista, 2018d).

En lo que respecta a iniciativas nacionales para enfrentar este fenómeno, en países como Brasil ya se cuenta con una ley de datos personales[15] que con base en el ejemplo europeo, pretende abordar los retos propios de la era digital. En contraste, en el caso de Colombia aún no contamos con iniciativas exitosas que busquen adaptar el régimen de protección de datos personales a la era del *big data* y la economía digital.[16] En vista de eso, en el presente documento pretendemos explorar: i) si en nuestro país los riesgos destacados por el Grupo de Trabajo del Artículo 29 son también latentes; y, en caso de serlo, ii) si nuestro régimen actual de protección de

---

14 OEA. *Informe del Comité Jurídico Interamericano. Privacidad y protección de datos personales.* 86° Periodo Ordinario de Sesiones. CJI/doc. 474/15 rev.2, adoptado el 26 de marzo de 2015, p. 1.

15 Ver Ley 13.709, del 14 de agosto de 2018.

16 La última iniciativa en la materia fue el Proyecto de Ley 106 de 2015, que modificaba el ámbito de aplicación de la Ley Estatutaria de Datos Personales para hacerla aplicable a responsables o encargados del tratamiento que a pesar de no residir ni estar domiciliados en el territorio de Colombia, realizaran cualquier operación o conjunto de operaciones sobre datos personales de personas que residieran, estuvieran domiciliadas o ubicadas en Colombia. Sin embargo, dicho proyecto fue finalmente retirado por su propio autor.

datos personales[17] y las autoridades competentes en la materia están preparados para enfrentarlos.[18]

Para el efecto, en el presente texto analizamos la forma de operar de una muestra de 30 EMNBD que recolectan datos en Colombia. Tal y como se expone más adelante, como principal criterio de selección de las empresas utilizamos lo que aquí denominamos su "grado de consolidación", clasificándolas como "grandes empresas de internet", "empresas intermedias," *start-ups* y "empresas establecidas". A partir de esta selección, y con base en una minuciosa revisión de las políticas de privacidad[19]

---

17 Por régimen de protección de datos nos referimos aquí a la implementación del artículo 15 de la Constitución Política y de las Leyes 1266 de 2008 y 1581 de 2012, así como de sus decretos reglamentarios 1377 de 2013 y 886 de 2014, que fueron luego incorporados al Decreto único 1074 de 2015.

18 Las autoridades competentes en materia de protección de datos personales a las que hacemos referencia son la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, en su calidad de autoridad de protección de datos, y los jueces de la República, encargados de velar por la garantía judicial del derecho.

19 Entendidas como los "documentos que explican cómo una organización maneja cualquier información de sus clientes, proveedores o empleados que haya reunido en sus operaciones" (Search Data Center, s. f.). Al respecto es preciso destacar que, en Colombia, a las políticas de privacidad se les denomina legalmente "políticas de tratamiento de información". De acuerdo con el artículo 25 de la Ley 1581 de 2012, estas políticas "obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley". Además, el Decreto 1377 de 2013, en su artículo 13, establece que este documento debe cumplir con el deber de informar, en un lenguaje claro y sencillo, por lo menos, lo siguiente:

"1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.

2. *Tratamiento* al cual serán sometidos los datos y *finalidad* del mismo cuando esta no se haya informado mediante el aviso de privacidad.

3. Derechos que le asisten como Titular.

4. Persona o área responsable de la atención de peticiones, consultas y reclamos, ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.

6. Fecha de entrada en vigencia de la política de tratamiento de la información y periodo de vigencia de la base de datos" (énfasis agregado).

(Anexo 1) de los principales productos ofrecidos por cada una de estas 30 empresas,[20] categorizamos la forma de operar de las 30 EMNBD seleccionadas. Lo anterior, utilizando las siguientes cuatro categorías de análisis: i) fuente de datos, ii) tratamientos, iii) finalidades de tratamiento, y iv) relación con Gafam. Una vez hecho esto, identificamos varias prácticas –propias de la era digital– que no han sido suficientemente contempladas por el régimen de datos personales actualmente aplicable en Colombia, y cuya regulación, en comparación con el GDPR europeo y con el CCPA de California, posee un amplio campo de mejora. Asimismo, identificamos varias falencias en las capacidades de las autoridades de protección de datos colombianas para hacer rendir cuentas a las EMNBD, y se proponen, en consecuencia, algunas medidas correctivas.

Esperamos que el contenido de este documento sea útil para los legisladores y hacedores de política pública que deben garantizar que el régimen de protección de datos personales colombiano continúe vigente en el marco de la era digital. Además, para los jueces y para la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, que desde sus distintos roles deben hacer efectivos los derechos a la intimidad y a la protección de datos de los titulares de los datos personales que hoy son masivamente recolectados en Colombia por parte de las EMNBD, o que son recolectados fuera del país pero con efectos domésticos. Esto, sin perjuicio de que su contenido pueda resultar también provechoso para las EMNBD, así como para los miembros de la sociedad civil, la academia y la ciudadanía en general que estén interesados en la protección de datos personales en la era digital.

20 Las políticas de privacidad deben diferenciarse de los llamados "términos y condiciones" o "términos de uso", en los que se establecen las reglas y los estándares generales de uso de la aplicación o del sitio web, incluyendo: información sobre derechos de autor, usos permitidos y prohibidos, condiciones de pago, responsabilidad del propietario de la aplicación o sitio web, entre otros. Así, si bien los "términos y condiciones" o "términos de uso" pueden hacer referencia a las políticas de privacidad, no son lo mismo. Ver Terms Feed (2018).

Aclaraciones previas sobre el alcance

Antes de pasar a desarrollar el contenido del texto consideramos pertinente hacer tres aclaraciones.

Por un lado, queremos dejar claro que en el presente documento los ejemplos del GDPR europeo y del CCPA de California no se sugieren como los modelos que necesariamente se deben seguir en Colombia. Por el contrario, los mismos solo se utilizan como guías o derroteros de las posibles soluciones por adoptar. Además, se traen a colación como evidencia de que tanto los conceptos como la regulación de protección de datos personales de la era predigital tienen potencial de mejorar y pueden evolucionar.

Por otro lado, somos conscientes de que, por sí sola, la regulación nacional no es suficiente. Lo anterior, en la medida en que, a diferencia del petróleo, que está enterrado y claramente localizado, los datos son un activo difuso, que se genera en todas partes y traspasa fácilmente las fronteras. En esa medida, y tomando como ejemplo el caso de la Unión Europea, el estado ideal parece ser el de una regulación al menos regional, que en el caso latinoamericano podría impulsarse desde instancias tales como la Comunidad Andina de Naciones (CAN) o la Comisión Interamericana de Derechos Humanos a través del sistema interamericano de derechos humanos. En nuestra opinión, a diferencia de la regulación local, una regulación de tal tipo le permitiría a los Estados latinoamericanos regular un mercado más grande, y, en esa medida, contar con un mayor poder de negociación frente a las EMNBD. Sin embargo, y dado que las iniciativas regionales están aún lejos de ser una realidad, en el presente documento optamos por comenzar con un abordaje nacional que le apunta, al menos, a mantener la protección de los derechos de los titulares de los datos personales recolectados en Colombia.

Finalmente, y gracias a los aportes recibidos en el grupo focal realizado el 20 de noviembre de 2018 con motivo de la publicación de este documento,[1] también somos conscientes de que la regulación estatal no es la única solución disponible para enfrentar los retos que el *big data* plantea para los derechos humanos; más aún, en un contexto de alta complejidad técnica, y en el que el desarrollo del derecho se queda corto frente al rápido avance de la tecnología. Así, además de la intervención estatal, existen medidas de autorregulación[2] que pueden adoptar –y ya están adoptando– las mismas EMNBD para asegurar de manera complementaria la protección de los derechos de los titulares de los datos personales. Incluso, se podrían aceptar las dinámicas propias del modelo de Estado regulador, en el que "*el derecho administrativo tiende a ser una regulación de la autorregulación*, de constatación de cumplimiento de las reglamentaciones privadas a las cuales el Estado atribuye efectos vinculantes" (Restrepo, 2009, p. 72) (énfasis agregado). Así, se podría pensar en la adopción de códigos de autorregulación aprobados por la autoridad de protección de datos, así como en firmas certificadoras de su cumplimiento por parte de las EMNBD. Del mismo modo, se pueden impulsar iniciativas de alfabetización digital de la ciudadanía, así como de capacitación de los científicos de datos en el procesamiento responsable de estos, para asegurar la protección de los derechos de los titulares.

A pesar de ello, y sin desestimar el valor de estas soluciones complementarias, consideramos que la intervención del Estado en esta materia no puede ser descartada, teniendo en cuenta: i) que la complejidad técnica de lo que se va a regular no es óbice para que el legislador y el ente regulador se puedan asesorar de técnicos en la materia, tal y como ya lo hacen en temas igualmente complejos como, por ejemplo, la regulación

---

1 La lista de asistentes al grupo focal puede encontrarse en el Anexo 3 de este documento.

2 Con base en la definición aportada por la Red Iberoamericana de Protección de Datos, la Corte Constitucional (Sentencia C-748 de 2011, M. P. Jorge Ignacio Pretelt Chaljub) ha definido la autorregulación como "las reglas adoptadas por las entidades para definir sus políticas y compromisos relativos al tratamiento de los datos personales" (Red Iberoamericana de Protección de Datos, 2006). Por su parte, la Comisión Europea se ha referido a la autorregulación como el conjunto "de normas que se aplican a una pluralidad de responsables del tratamiento que pertenezcan a la misma actividad profesional o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión" (Comisión Europea, 1998).

del espectro radioeléctrico y el espectro electromagnético; ii) que el alto poder económico, tecnológico y social que han adquirido las grandes empresas de internet genera fallas de mercado que llaman al Estado a intervenir para "procurar que el mercado funcione adecuadamente en beneficio de todos, no de quienes dentro de él ocupan una posición especial de poder, en razón a su predominio económico o tecnológico";[3] y, iii) que es el Estado, y no las empresas, el principal encargado de velar por la protección de los derechos humanos de sus ciudadanos.

Frente a este último punto resulta preciso recordar que el derecho a la protección de datos personales constituye un derecho humano, el cual ha sido reconocido en varios instrumentos del derecho internacional de los derechos humanos. Por un lado, en el caso del Sistema Universal de Protección de Derechos, el derecho a la protección de datos personales ha estado íntimamente atado al derecho a la intimidad, consagrado en el artículo 12 de la Declaración Universal de Derechos Humanos, y luego reproducido en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). A partir de dichos preceptos, en 1998 el Comité de Derechos Humanos adoptó la Observación General No. 16 sobre el Derecho a la intimidad, en la que estableció que:

> … para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación.

Asimismo, en el seno de las Naciones Unidas han surgido iniciativas tales como los Principios Rectores Aplicables a los Ficheros Computarizados de Datos Personales[4] y la Resolución de las Naciones Unidas

---

3 Corte Constitucional, Sentencia C-150 de 2003, M. P. Manuel José Cepeda Espinosa.

4 Los Principios Rectores Aplicables a los Ficheros Computarizados fueron aprobados mediante Resolución A/Res/45/95 de la Asamblea General de las Naciones Unidas, tomando como modelo las directrices de la Organiza-

sobre el Derecho a la Privacidad en la Era Digital.[5] En lo que respecta al sistema interamericano de derechos humanos, el derecho a la protección de datos personales es interpretado a partir del artículo 11 de la Convención Americana sobre Derechos Humanos (CADH). Además, dentro de los documentos más recientes en la materia se encuentra la Resolución de la Asamblea General AG/RES.2842 (XLIV-O/14) sobre Acceso a la Información Pública y Protección de Datos Personales, mediante la cual se reafirma la importancia de la protección de los datos personales y del respeto al derecho a la privacidad. Adicionalmente, y después de que la Asamblea General resolviera encomendarle la formulación de propuestas de distintas formas de regular la protección de datos personales, el Comité Jurídico Interamericano ha emitido algunos documentos relevantes en la materia, entre los que se destacan: Privacy and Data Protection CJI/doc. 465/14; Privacidad y Protección de Datos CJI/doc. 450/14; y Privacidad y Protección de Datos Personales CJI/doc.474/15 rev.2.

En esa medida, si bien este derecho debe ser respetado por todos, es claro que la obligación de su garantía pesa principalmente sobre el Estado.

---

ción para la Cooperación y Desarrollo Económicos (OCDE). Dentro de los principios se encuentran: el de licitud y lealtad, exactitud, finalidad, acceso de la persona interesada, no discriminación, seguridad, entre otros.

5 La Resolución de las Naciones Unidas sobre el Derecho a la Privacidad en la Era Digital A/C.3/71/L.39 trae exhortaciones tanto a los Estados como a las empresas. A los Estados específicamente los exhorta a respetar y proteger el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales; a adoptar medidas para prevenir y poner fin a la violación de este derecho; a examinar procedimientos, prácticas y legislación relativos a vigilancia e interceptación de comunicaciones, así como a mantener mecanismos nacionales de supervisión; a proporcionar acceso a recursos efectivos a las personas cuyo derecho a la privacidad haya sido violado; a elaborar y aplicar una legislación adecuada para proteger a las personas de tratamientos ilegales y arbitrarios, especialmente cuando se toman decisiones basadas en el tratamiento automatizado la retención o el uso de datos personales por particulares, empresas y organizaciones privadas.

MUESTRA DE EMPRESAS CON MODELOS DE NEGOCIO BASADOS EN DATOS (EMNBD) QUE RECOLECTAN DATOS EN COLOMBIA

Como se adelantó más arriba, como criterio de selección de la muestra de 30 EMNBD cuya forma de operar será analizada en este documento, se utilizó el grado de consolidación de la empresa, y se crearon las siguientes cuatro categorías: i) grandes empresas de internet; ii) empresas intermedias; iii) *start-ups*; iv) empresas establecidas.

En lo que respecta a las grandes empresas de internet, la muestra incluye a las cinco empresas comúnmente agrupadas con el acrónimo Gafam, quienes se destacan por su capacidad de innovación y amplio capital de inversión (Corporación Colombia Digital, 2013). Por su parte, en el otro extremo incluimos empresas comúnmente denominadas como *start-ups*, es decir, aquellas que se definen por su temprana edad, escalabilidad y crecimiento exponencial (Entrepreneur, 2018). En el medio de estas dos categorías se encuentran las aquí denominadas "empresas intermedias", en la medida en que ya no se encuentran en una etapa temprana para ser consideradas *start-ups*, pero tampoco han alcanzado aún el nivel de consolidación de las grandes empresas de internet. Finalmente, la categoría de "empresas establecidas" incluye aquellas que, a diferencia de las que conforman las demás categorías, surgieron antes de la era digital, pero que han adaptado sus modelos de negocio al *big data*, o han creado nuevos modelos de negocio basados en datos.

Dado que se trata de las empresas que recolectan datos en Colombia, como criterio de selección de las "empresas intermedias" se tuvo en cuenta el *ranking* de la empresa de información y mercado de aplicaciones App Annie,[1]

1 App Annie. *Top App Matrix*. Disponible en https://www.appannie.com/das-

sobre las aplicaciones más descargadas en Colombia en AppStore (iPhone Top App Matrix) (Anexo 4) y Google Play (Google Play Top App Matrix) (Anexo 5). Al revisar las aplicaciones más descargadas en esos dos sitios web en los primeros cinco días de los meses de julio, agosto y septiembre,[2] y tabular esa información, los resultados son los de la tabla 1.

Como se ve, de las 16 *Apps* más descargadas en Colombia, 9 (56%) son propiedad de las Gafam (WhatsApp, Messenger, Facebook,

TABLA 1

Ranking* de las aplicaciones que más aparecen en el top 10 de aplicaciones más descargadas en Colombia en los primeros cinco días de los meses de julio, agosto y septiembre de 2018

APP	Veces que aparece en el top 10 de las más descargadas en Colombia	EMNBD a la que pertenece
WhatsApp	30	Facebook Inc.
Tinder	30	Match Group, LLC.
Messenger	24	Facebook Inc.
Facebook	23	Facebook Inc.
Instagram	17	Facebook Inc.
Facebook Lite	15	Facebook Inc.
Netflix	15	Netflix International B.V.
Deezer	15	Deezer SA
Google Drive	15	Google LLC.
YouTube	13	Google LLC.
Linkedin	10	Microsoft Corporation
Messenger Lite	2	Facebook Inc.
AliExpress	2	Alibaba Group
Joom	1	SIA Joom (Latvia)
30 Days Fitness Challenge	1	Bending Spoons S.p.A.
8fit Workouts and Meal Planner	1	Urbanite Inc.

* De dichos resultados se excluyeron tanto las aplicaciones de juegos, como las aplicaciones de DirectTV y Selección Colombia que fueron masivamente descargadas por el Mundial Rusia 2018.

FUENTE: elaboración propia a partir de información disponible en la página web de la empresa de información y mercado de aplicaciones App Annie.

hboard/home/

2 Si bien se pretendía cubrir un rango mayor de días, la versión gratuita de la página web de App Annie solo nos permitió acceder a esa información.

Instagram, Facebook Lite, Google Drive, YouTube, LinkedIn y Messenger Lite). Sin embargo, existen otras 7 empresas que, al ser propietarias de otras de las aplicaciones más descargadas, entran dentro de nuestro grupo de "empresas intermedias". Asimismo, se agregaron otras cuatro empresas cuyas aplicaciones (Spotify, Waze, Uber y EasyTaxi), si bien no están dentro del top 10 de las más descargadas en los últimos tres meses, son bastante populares en el país.

En lo que respecta a los *start-ups*, el criterio de selección de la muestra fue su adscripción a Team Startup Colombia o al portafolio de *start-ups* dinámicas creado por INNpulsa Colombia. El primero es un grupo de emprendimientos digitales, que según el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC, s. f.), "por sus buenas prácticas, logros, tracción, ventas, crecimiento, inmersión en nuevos mercados, inversión, entre otros, están a nivel de importantes *start-ups* mundiales y son referente para los colombianos a nivel nacional e internacional". Por su parte, el segundo es un portafolio de emprendimientos que según INNpulsa Colombia (s. f.),[3] son los mejores *start-ups* para invertir en el país. Al respecto, se aclara que en esta muestra no fueron incluidas todas las empresas que hacen parte de esos dos portafolios, sino solo aquellas que aún siguen existiendo y para las cuales fue posible encontrar su política de privacidad. Igualmente, se agregaron otras dos empresas más que si bien no están adscritas a ninguno de esos portafolios, ofrecen aplicaciones (Biko y Duety) con modelos de tratamiento de datos que resulta interesante estudiar.

Por último, para escoger entre las "empresas establecidas" se decidió seleccionar a las empresas más grandes que existen en Colombia en cada uno de los siguientes sectores: consumo masivo, *retail* (Portafolio, 2017), seguros (BNamericas, 2017), financiero (El Tiempo, 2017) y de telecomunicaciones (La República, 2018).

Siendo así, la muestra de 30 EMNBD que es objeto de estudio en este documento quedó conformada como se observa en la tabla 2.

Evidentemente, se trata de una muestra de EMNBD que no pretende ser representativa, sino meramente ilustrativa del tipo de empresas que están recogiendo datos en Colombia actualmente. Con seguridad se quedan por fuera múltiples empresas que hacen tratamiento de datos dignos

3 INNpulsa Colombia es la agencia del Gobierno colombiano que busca activar el crecimiento empresarial extraordinario a través de la innovación.

TABLA 2
Muestra de EMNBD objeto de estudio

Categoría	EMNBD	Productos*	Descripción
Grandes empresas de internet (5)	Google LLC.	Google Search Google Drive Google Maps YouTube	Compañía cuya especialización son los productos y servicios relacionados con internet, software, dispositivos electrónicos y otras tecnologías.
	Amazon Inc.	Amazon.com	Compañía de comercio electrónico y servicios de computación en la nube.
	Facebook Inc.	Facebook Facebook Lite Messenger Messenger lite Instagram WhatsApp (con política de privacidad propia)	Compañía que ofrece servicios de redes sociales y medios sociales en línea.
	Apple Inc.	Iphone Ipad Apple Watch ICloud	Compañía que diseña y produce equipos electrónicos, software y servicios en línea.
	Microsoft Corporation	Windows Office 365 Microsoft Azure Microsoft Dynamics 365 Microsoft Intune Windows Server SQL Server Visual Studio System Center StorSimple Bot Framework Cortana Skills Kit Botlet Store Bing Cortana Microsoft Translator SwiftKey Xbox MSN Mixer Microsoft Store Silverlight Outlook LinkedIn (con política de privacidad propia)	Compañía que ofrece servicios, sitios web, aplicaciones, software, servidores y dispositivos.

Categoría	EMNBD	Productos*	Descripción
Empresas intermedias (11)	Match Group, LLC.	Tinder	Compañía que proporciona una aplicación geosocial que permite a los usuarios comunicarse con otras personas con base en sus preferencias para charlar y concretar citas o encuentros.
	Netflix International B.V.	Netflix	Empresa de entretenimiento que proporciona, mediante tarifa plana mensual, un streaming de contenido multimedia bajo demanda por internet.
	Deezer SA	Deezer	Sitio web y aplicación que, mediante una suscripción, ofrece música de manera ilimitada.
	Alibaba Group	AliExpress	Tienda en línea que ofrece productos de pequeñas empresas de China y de otros lugares para compradores internacionales.
	SIA Joom (Latvia)	Joom	Tienda en línea que ofrece productos chinos a muy bajos precios.
	Bending Spoons S.p.A.	30 Days Fitness Challenge	Aplicación de fitness para hacer entrenamiento en casa.
	Urbanite Inc.	8fit Workouts and Meal Planner	Aplicación de fitness que funciona como un entrenador físico personal, preparando el entrenamiento personal y el plan nutricional del usuario en función de los objetivos de entrenamiento autodefinidos.
	Spotify AB	Spotify	Compañía que proporciona una aplicación multiplataforma empleada para la reproducción de música vía streaming.
	Waze Mobile Limited	Waze	Compañía que proporciona a sus clientes una aplicación social de tránsito automotor en tiempo real y navegación asistida por GPS.
	Uber B.V.	Uber	Compañía que proporciona a sus clientes una red de transporte privado, a través de su software de aplicación móvil, que conecta los pasajeros con los conductores.
	Easy Taxi Colombia S.A.S.	Easytaxi	Aplicación que permite a sus usuarios solicitar un servicio de taxi y rastrearlo en tiempo real.

Categoría	EMNBD	Productos*	Descripción
Start-ups (9)	1DOC3 S.A.S.	1DOC3	Plataforma web en la que médicos responden inquietudes de salud de manera anónima y gratuita.
	Acsendo S.A.S	Ascendo	Software en la nube que ayuda a evaluar el clima laboral y desempeño de las organizaciones.
	Fluvip S.A.S	Fluvip	Plataforma virtual que conecta grandes marcas con influenciadores alrededor del mundo, permitiendo identificar los influenciadores adecuados para cada campaña y marca.
	Rappi S.A.S	Rappi	Aplicación que ofrece una gama ancha de productos y servicios disponibles para la entrega, mediante el uso de "rappitenderos".
	Cívico Digital S.A.S	Cívico	Plataforma virtual en la que los ciudadanos construyen su ciudad compartiendo información a través de misiones, en las cuales acumulan puntos que luego pueden canjear por beneficios.
	Inversiones CMR S.A.A	Domicilios.com	Pedidos online a través de la web o de aplicaciones móviles.
	IoT Services Inc.	Ubidots	Plataforma basada en una nube que integra información proveniente de diferentes fuentes y ayuda en el proceso de dar sentido a la información recogida.
	Biko Development Inc.	Biko	Aplicación móvil que busca incentivar el uso de las bicicletas en las ciudades, al recompensar a sus usuarios con un sistema de puntos redimibles en bienes y servicios.
	Duety S.A.S	Duety	Red social para que las parejas hagan "matripuntos".
Empresas establecidas (5)	Unilever PLC Unilever N.V.	Grupo Unilever	Multinacional de consumo masivo que produce y vende productos bajo el nombre de 400 marcas a nivel mundial.
	Almacenes Éxito S.A.	Grupo Éxito	Multinacional de retail.

Categoría	EMNBD	Productos*	Descripción
Empresas establecidas (5)	Seguros Generales Suramericana S.A.	SURA	Compañía de seguros.
	Grupo Aval Acciones y Valores S.A.	Grupo Aval	Conglomerado empresarial colombiano dedicado a una amplia variedad de actividades, principalmente financieras.
	Telmex Colombia S.A.	Claro	Empresa de servicios de telecomunicaciones.

* Esta lista de productos es meramente enunciativa, y no pretende ser exhaustiva de la totalidad de los productos ofrecidos por cada EMNBD.
FUENTE: elaboración propia.

de ser analizados. Sin embargo, y tal y como se verá a continuación, la forma de operar de las empresas aquí incluidas ya permite abordar con suficiente riqueza el debate sobre el grado de preparación de nuestro régimen legal de protección de datos y de las autoridades competentes para enfrentar la era digital.

FORMA DE OPERAR DE LAS EMNBD QUE RECOLECTAN DATOS EN COLOMBIA

A partir de la revisión de las políticas de privacidad de los productos ofrecidos por las 30 EMNBD que hacen parte de la muestra (Anexo 1), a continuación pasamos a caracterizar su forma de operar. Lo anterior, con base en las siguientes cuatro categorías de análisis: i) fuente de datos, ii) tratamientos, iii) finalidades de tratamiento, y iv) relación con Gafam. Como se verá, la descripción de estas categorías combina vocabulario tanto de la terminología propia de la protección de datos personales, como de la terminología comúnmente utilizada para caracterizar a los modelos de negocio basados en datos (Hartmann *et al.*, 2014; Alcaíno *et al.,* 2015) (al respecto, ver Anexo 2).

Fuentes de datos

La mayoría de las EMNBD objeto de la muestra tienen las siguientes tres fuentes de datos: i) los datos proporcionados por el usuario/cliente; ii) los datos recolectados a través de *web tracking*;[1] y, iii) los datos proporcionados por "socios estratégicos".

En lo que respecta a los *datos proporcionados por el usuario/cliente* se trata usualmente de información que este proporciona al crear una cuenta o perfil (v. gr. nombre, contraseña, número de teléfono), usar el servicio (v. gr. ubicación de destino), hacer una compra (v. gr. ítems adquiridos, datos de pago, cuentas bancarias) o al subir contenido a la plataforma o aplicación. Sin embargo, frente al contenido subido resulta digno de destacar el

1 Mecanismo de rastreo que permite identificar las herramientas que utilizamos en internet, tales como el dispositivo, la red Wifi, el tipo de navegador, entre otras.

caso de la aplicación WhatsApp, cuya política de privacidad especifica que salvo en circunstancias excepcionales,[2] el contenido de los mensajes que el usuario envía por medio de la aplicación no se guarda en los servidores de Facebook Inc., sino en el dispositivo del usuario. En forma similar, en la política de privacidad de la aplicación 30 Days Fitness Challenge se señala: "note que el proveedor de la aplicación no almacena ninguna información respecto a lo que usted escribe, mientras utiliza la aplicación".

En algunos casos, como Facebook, Tinder, 1DOC3, Unilever o Sura, la información proporcionada por el usuario/cliente incluye datos sensibles (también llamados "datos con protección especial" o "categorías especiales de datos personales"), como creencias religiosas, ideologías políticas, intereses o aspectos relacionados con la salud, origen étnico o racial, creencias filosóficas, afiliación sindical, plantilla de reconocimiento facial. En otros casos, como el de AliExpress, el suministro de esa información es opcional, y aclara que "si prefiere no proporcionar dicha información, el uso de nuestros servicios y productos no se verá afectado". Por su parte, en el caso de Unilever, en su política de privacidad se señala que "en algunos casos, es posible que haya solicitado servicios o productos que no impliquen directamente la recopilación de categorías especiales de datos, pero pueden implicar o sugerir su religión, salud u otras categorías especiales de datos". En contraste, otras empresas, como es el caso de Ascendo, aclaran expresamente que "no recolectan, almacenan, organizan, usan, circulan, transmiten, transfieren, actualizan, rectifican, suprimen, eliminan y gestionan datos sensibles". En forma similar, en la política de privacidad de EasyTaxi se lee: "Ninguno de los datos que serán objeto de tratamiento tienen el carácter de dato sensible".

Frente a los *datos recolectados a través de web tracking*, estos incluyen normalmente datos sobre las aplicaciones, los navegadores y los dispositivos que utiliza el usuario/cliente (la llamada *log data*) (v. gr. la dirección IP, versión y tipo de dispositivo y navegador, configuración de zona horaria, preferencias de idioma, tipos y versiones de complementos de su navegador, proveedor de servicios de internet –ISP–, velocidad de la conexión), y sobre su actividad en la respectiva plataforma o aplicación (la

2 A saber: i) si un mensaje no puede entregarse de inmediato, pueden guardarlo en sus servidores hasta por 30 días mientras intentan entregarlo. Si un mensaje no se ha entregado después de 30 días, lo eliminan; ii) si muchas personas comparten una foto o un video popular, pueden conservar dicho contenido en sus servidores durante un periodo más prolongado.

llamada *online data*) (v. gr. las horas y fechas de acceso a los servicios, productos que ha visitado o que ha buscado, detalles de compras, los *hashtags* utilizados, las personas y los grupos con los que interactúa, *clics* del *mouse*, desplazamiento por la página o número de veces que pasa el *mouse* por encima de determinados elementos, la URL de la que proviene, formas de salir de la página web y la URL a la que accede seguidamente). Asimismo, incluyen datos sobre la ubicación del usuario/cliente (incluso cuando la aplicación no está en uso), la cual puede ser determinada a partir del GPS, dirección IP, datos del sensor del dispositivo utilizado, puntos de acceso a Wifi, antenas de servicio de telefonía móvil o dispositivos con Bluetooth activado que están cerca de este, u otros dispositivos que se encuentran cerca o que comparten la red. Sin embargo, y como ejemplo a nuestro parecer replicable, en el caso de Apple en su política de privacidad se aclara que "a menos que proporciones tu consentimiento, estos datos sobre la ubicación se recolectan de forma anónima en una forma que no te identifica personalmente".

Resulta preocupante notar que, a diferencia de los datos proporcionados por el usuario/cliente, algunas empresas –como Duety y Apple– consideran que los datos recolectados a través de *web tracking* son *información no personal,* pues no están vinculados con el usuario/cliente sino con las direcciones de Protocolo de Internet (IP) y los identificadores similares del dispositivo utilizado. Por ejemplo, Duety señala: "no tratamos el Log Data como información personal ni la usamos en asociación con otra información personal, sin embargo, podríamos agregarla, analizarla y evaluarla con los mismos propósitos declarados más arriba para la información personal no identificable". No obstante, en el caso de Apple, se aclara que se tratarán las direcciones IP y los identificadores similares como información personal "cuando estos sean así considerados en la legislación local".

Por su parte, y de forma más garantista para el derecho a la protección de datos personales de sus usuarios, Cívico señala que:

> … aunque tratamos esta información como datos personales, es importante que usted sepa que *CÍVICO solamente utiliza estos datos en forma global,* es decir, para informarle a nuestros socios y aliados sobre la manera en que nuestros usuarios, *colectivamente considerados,* utilizan nuestros servicios, de manera que nuestros socios también puedan comprender con qué frecuencia las personas utilizan sus servicios y nuestros servicios (énfasis agregado).

En forma similar, en la política de privacidad de la aplicación 8fit Workouts and Meal Planner se señala:

> ... hacemos notar que de los datos recopilados no podemos y no intentamos sacar ninguna conclusión sobre su identidad. La dirección IP de su dispositivo y la otra información mencionada anteriormente son utilizados por nosotros para los siguientes propósitos: para garantizar que se pueda establecer una conexión sin problemas; para garantizar el uso conveniente de nuestros servicios; para evaluar la seguridad y la estabilidad del sistema; otros fines administrativos.

En contraste, LinkedIn reconoce claramente que "utilizamos registros de inicio de sesión, información de dispositivos y direcciones de protocolo de internet (IP) para identificarte y registrar tu uso en LinkedIn".

En relación con los *datos proporcionados por socios estratégicos*, las fuentes son menos homogéneas, siendo las más comunes: i) los terceros que prestan algún servicio en nombre de la empresa (v. gr. transportistas); ii) las empresas de *marketing* o anunciantes que les proporcionan servicios publicitarios y de investigación (en cuyo caso pasan los detalles sobre el éxito de una campaña en sitios web propios o de terceros); iii) las plataformas de terceros en las que la empresa tiene cuentas, como cuando los usuarios utilizan la función "Me gusta" en Facebook o la función +1 en Google+; iv) los llamados "third-party data enrichment providers" que procesan y sacan conclusiones sobre los datos personales en poder de las EMNBD; v) las empresas a las que ellos les proporcionan servicios, como en el caso de Google, los sitios web que usen servicios de publicidad como AdSense, incluyen herramientas de análisis como Google Analytics o incorporan contenido de video de YouTube; o, en el caso de Uber, quienes utilicen la API de Uber; y, vi) los burós de crédito que utilizan las aplicaciones y plataformas para ofrecer servicios de crédito y financieros a determinados usuarios/clientes.

Frente a ese intercambio de datos, varias de las empresas, como Facebook y Fluvip, exigen que todos los terceros cuenten con derechos legítimos para recopilar, usar y compartir esa información. Por el contrario, Spotify señala que "utilizaremos estos datos personales, ya sea que haya proporcionado su consentimiento al tercero o a Spotify para ese intercambio de datos *o cuando Spotify tenga un interés legítimo* para utilizar los datos personales para proporcionarle el Servicio de Spotify" (énfasis agregado). Por su parte, WhatsApp advierte: "protegemos los datos obtenidos de

terceros de acuerdo con las prácticas que se detallan en esta declaración, además de las restricciones adicionales impuestas por la fuente de los datos".

Además de estas tres fuentes de datos, se identificó la *adquisición de información de proveedores de datos externos* (Acxiom, Oracle, etc.) como una cuarta fuente, aunque menos utilizada (o al menos explicitada en las políticas de privacidad). También llamados "proveedores de datos *online* y *offline*", se trata de terceros que les venden datos sobre las acciones y las compras que hacen los usuarios/clientes dentro y fuera de internet. Sin embargo, no es tan claro si estos *data brokers* solo les entregan información estadística y demográfica agregada que pueden atribuirle a los usuarios con base en su asignación en ciertos grupos estadísticos o de uso de servicios, o si también les entregan datos personales que permiten individualizar al titular. Por ejemplo, en su política de privacidad Biko reconoce "la compra [de] datos de *marketing* de terceros", sin que sea claro si se trata de datos granulares o agregados. En forma más clara, Microsoft señala que una de sus fuentes son los "agentes de datos a los que compramos datos demográficos para complementar los datos que recopilamos". De igual forma, tampoco es claro a título de qué se transfieren esos datos de terceros. Por ejemplo, en el caso de Facebook, en su política de privacidad se señala:

> Facebook colabora con un selecto grupo de proveedores de datos de terceros para ayudar a los negocios a conectarse con las personas que podrían estar interesadas en sus productos o servicios. […] Son muchos los negocios que hoy en día trabajan con terceros como Acxiom, Oracle Data Cloud (antes DLX), Epsilon, Experian y Quantium con el fin de administrar y analizar las iniciativas de *marketing*. […] El tercero *proporciona* información a Facebook para que la plataforma conecte a los clientes con las ofertas. (Énfasis agregado)

Además, allí se dice que los proveedores de datos de Facebook se comprometieron a facilitar un formulario de exclusión en sus sitios web, para no recibir publicidad personalizada a partir de esos datos. Sin embargo, entre los *links* de formularios disponibles no se encuentra ninguno para Colombia.

Por último, algunas de las empresas incluidas en la muestra utilizan también, aunque en mucha menor medida, *datos de libre acceso en la web* (Google –*web crawling*,[3] Apple– fuentes de acceso público, Fluvip –redes

3 Utilización de programas informáticos que navegan la web e indexan con-

sociales, y Netflix y Microsoft– bases de datos gubernamentales abiertas), *sensores y dispositivos* (Ubidots, Biko) y *crowdsourcing*[4] (Facebook, Cívico, Waze).

Tratamientos

Los tratamientos de datos personales adelantados por las EMNBD objeto de la muestra parecen ser uniformes, centrándose principalmente en las siguientes actividades: recolección y análisis.

En lo que respecta a la *recolección*, esta suele realizarse a través de las siguientes herramientas tecnológicas: i) *cookies de origen o de terceros:* archivos pequeños que contienen una cadena de caracteres que se envían al computador del usuario cuando visita un sitio web. Cuando vuelve a visitar el sitio, la *cookie* permite que ese sitio reconozca su navegador. Las *cookies* pueden almacenar las preferencias del usuario y otro tipo de información; ii) *identificadores de anuncios*: son similares a las *cookies* pero se encuentran en varios dispositivos móviles y tabletas (por ejemplo, el "identificador para anunciantes", o IDFA, de los dispositivos con Apple iOS, y el "identificador de anuncios de Google" en los dispositivos con Android), y en algunos reproductores multimedia; iii) *etiquetas de pixel* (*web beacons*, *clear.gif* o señalizaciones web): un tipo de tecnología presente en un sitio web o en el interior del cuerpo de un correo electrónico, que permite realizar un seguimiento de cierta actividad como las visitas de un sitio web o cuándo se abre un correo electrónico; iv) *kits de desarrollo de software (SDK)*: pequeños fragmentos de código que se incluyen en las *apps* y funcionan como las *cookies* y las etiquetas de pixel; v) *almacenamiento web del navegador*: tecnología de almacenamiento local que permite que los sitios web almacenen datos en el navegador de un dispositivo; vi) *cachés de datos de aplicación:* repositorio de datos en un dispositivo que permite que una aplicación web se ejecute sin una conexión a internet, y que el contenido se cargue más rápido para mejorar el rendimiento de la aplicación; vii) *registros de servidor:* servidores de la EMNBD que registran automáticamente las solicitudes que realiza el usuario de las páginas

tenidos. Por ejemplo, es lo que utiliza la plataforma Google Search para arrojar resultados de búsqueda.

4 Construcción colectiva de información a través de la participación de la comunidad en diferentes tareas. Es el caso de la aplicación Waze, que tiene como una de sus fuentes de datos (combinada con el Web Tracking), el aporte de los usuarios sobre el estado de las vías y de los trancones.

cuando visita los sitios; y, viii) *direcciones URL de seguimiento*: enlaces personalizados que le ayudan a las empresas a comprender de dónde viene el tráfico de sus páginas web.

De hecho, empresas como Apple, 1Doc3, Biko, Tinder, Netflix y Microsoft especifican –a partir de la Guía de Cookies de la Cámara Internacional de Comercio del Reino Unido (salvo Microsoft, que provee otros nombres)– las clases de *cookies* que utilizan para recolectar información. Así, dentro el universo de estos archivos, las más comunes son: a) *cookies estrictamente necesarias*: son esenciales para que el usuario pueda navegar por los sitios web y usar sus funcionalidades; b) *cookies de análisis o de comportamiento:* permiten cuantificar el número de usuarios, cómo usan los sitios web y así realizar la medición y el análisis estadístico de la utilización que hacen los usuarios del servicio ofertado. Estos datos pueden usarse para ayudar a optimizar los sitios web y hacerlos más fáciles de navegar. Estas *cookies* también se usan para que los afiliados de la empresa sepan si los usuarios llegaron a alguno de sus sitios web desde un afiliado, y si su visita tuvo como resultado el uso o la compra de alguno de sus productos o servicios, incluidos los detalles del producto o del servicio adquirido; c) *cookies de funcionalidad:* con estas los sitios web pueden recordar las decisiones que toma el usuario mientras navega y reconocerlo cuando regresa. Por ejemplo, pueden almacenar la ubicación geográfica en una *cookie* para mostrarle al usuario el sitio web indicado para su región. También pueden recordar las preferencias, tales como el tamaño del texto, las fuentes y otros elementos configurables del sitio. También pueden usarse para hacer seguimiento de los productos o videos destacados que se han consultado, y así evitar repetirlos; d) *cookies publicitarias o dirigidas:* permiten analizar los hábitos de navegación en internet y, de esa manera, gestionar –con base en el perfil de navegación del usuario– la oferta de los espacios publicitarios que hay en las páginas web, adecuando el contenido del anuncio al contenido del servicio solicitado o al uso que realice el usuario de la página web; e) *cookies de interacción o de redes sociales*: también llamadas *plugins* sociales (como "Me gusta" de Facebook), estas permiten al usuario mostrar su interés por una página o recomendarla, y pueden recolectar información aun si el usuario no las utiliza. Al respecto, es interesante notar que Apple aclara que en el caso de las *cookies de análisis o de comportamiento* y de las *de funcionalidad*, "estas *cookies* no recolectan información que te identifique". Si bien consideramos que en principio esto es bueno, se debe tener en cuenta la posibilidad, siempre latente, de

que el titular de esos datos pueda ser finalmente identificado a partir de la combinación de varios datos aparentemente impersonales.

Por su parte, hay empresas como AliExpress, Duety, Tinder, o la propietaria de la aplicación 8fit Workouts and Meal Planner, que además utilizan las siguientes clasificaciones: a) *cookies permanentes/persistentes*: para guardar la información de Inicio de Sesión para futuros inicios de sesión; b) *cookies de identificación de sesión*: para habilitar ciertas características del sitio y la aplicación, a fin de entender mejor la forma en la que el usuario interactúa con el sitio y la aplicación, y monitorear el uso agregado de los usuarios y el tráfico web que llevó al sitio y a la aplicación. A diferencia de las *cookies* permanentes, las de sesión son borradas del computador del usuario cuando cierra sesión en el sitio web o en la aplicación. Además, Deezer reconoce el uso de *cookies de terceros* al señalar que "autoriza a ciertos socios comerciales a insertar herramientas de seguimiento publicitarias en los Servicios o en los anuncios mostrados. La inserción y el uso de herramientas de seguimiento están sujetos a las políticas de privacidad de dichos terceros".

En cuanto al *análisis*, el mismo es normalmente de tipo *descriptivo*, encaminado a segmentar a los usuarios y a las audiencias de acuerdo con gustos, intereses y conexiones, o *prescriptivo*, para mejorar la experiencia del usuario en futuras visitas. Y en lo que respecta a las herramientas tecnológicas para adelantar dichos análisis, el nivel de detalle encontrado en las políticas de privacidad es muy bajo, y en ocasiones nulo. Entre quienes proporcionan algo de información, empresas como Rappi hablan de "herramientas de inteligencia de negocios y minería de datos". En forma similar, Microsoft habla de "procesos automatizados" y AliExpress de "utilización de datos anonimizados para propósitos de *machine learning*". Por su parte, Google menciona Google Analytics y sistemas automatizados de análisis y algoritmos, mientras que Netflix habla de "algoritmos de recomendación". Con un mayor grado de especificidad, 1DOC3 y Ubidots se refieren al IBM Watson Natural Language Classifier service on IBM Bluemix, que categoriza las consultas de los usuarios en tiempo real, entregando contenido específico para preguntas repetidas y enviando nuevas solicitudes a personas reales. Por último, Unilever refiere que utiliza "simulaciones de juego de evaluaciones de comportamiento basadas en la ciencia y técnicas de ciencia de datos". Por útlimo, resulta interesante resaltar el caso de Apple, que evidentemente influenciado por el GDPR, en su política de privacidad aclara que "no toma decisiones sobre el *uso*

de algoritmos ni la *generación de perfiles* que pueden afectarte significativamente" (énfasis agregado).

Por último, la única empresa que reconoce abiertamente la *venta o comercialización de datos personales* es Cívico. En contraste, Amazon, Facebook, Joom, Uber y Waze señalan de manera expresa 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 estas empresas (salvo Joom), al igual que el resto de las aquí estudiadas, 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. Empero, cabe destacar que Google, Amazon, Ubidots, Spotify, Waze y LinkedIn, de manera positiva, garantizan que la información entregada al comprador continuará sujeta a los compromisos adquiridos en cualquier aviso de privacidad preexistente, hasta que se le notifique al usuario. Incluso, de manera más garantista, AliExpress y Netflix señalan que "en relación con una reorganización, reestructuración, fusión o venta, o cualquier otra transferencia de bienes, nosotros transferiremos la información, incluida la personal, a condición de que el destinatario se comprometa a respetar su información personal de conformidad con nuestra Declaración de privacidad".

Finalidades

Las finalidades más comunes con las que las EMNBD aquí estudiadas tratan los datos personales son: i) prestar un bien o servicio; ii) comunicarse e interactuar con el usuario; iii) desarrollar nuevos bienes o servicios a partir de la identificación de necesidades; iv) administrar sorteos, concursos, descuentos u otras ofertas; v) adelantar investigaciones de mercados; vi) *ofrecer contenidos personalizados (incluidos anuncios y publicidad)*; vii) medir el rendimiento de los contenidos; viii) elaborar estudios e investigaciones; ix) *compartir información con terceros.* En ese último caso, los posibles terceros con quienes se comparte información son: a) anunciantes; b) *empresas del mismo grupo o sociedades subsidiarias, filiales o aliadas*; c) *aplicaciones de terceros que se conectan a la aplicación de la empresa o que se utilizan para iniciar sesión en ella*; d) proveedores de servicios en su nombre; e) *investigadores académicos*; f) socios de medición; g) *autoridades públicas*; y, eventualmente, h) posibles compradores de la empresa.

Por su alto nivel de transparencia, es de notar el caso de la aplicación 8fit Workouts and Meal Planner, cuya política de privacidad incluye los nombres de las aplicaciones de terceros que se conectan a la aplicación o

que se utilizan para iniciar sesión en ella, así como de los socios de medición con los que se comparte información. Esto, en contraste con el resto de las EMNBD aquí estudiadas, que hablan genéricamente de "aplicaciones de terceros" y "socios de medición".

Asimismo, frente a las garantías proporcionadas para el intercambio de información con terceros resulta interesante el caso de WhatsApp, que a la hora de compartir la información del usuario con servicios de terceros y con las empresas de Facebook (grupo empresarial del que hace parte), señala: "cuando compartimos información con proveedores de servicios de terceros y las empresas de Facebook que actúan como tales, les exigimos que respeten nuestras instrucciones y cumplan con nuestras condiciones en el momento de usar tu información en nuestro nombre". En el mismo sentido, AliExpress dispone que "estos proveedores de servicios deben cumplir con nuestros requisitos de privacidad y seguridad de datos y solo se les permite usar sus Datos personales en relación con los fines especificados anteriormente, y no para sus propios fines". Por su parte, LinkedIn señala que:

> No compartiremos tus datos personales con ningún anunciante ni con redes publicitarias para su publicidad, excepto: i) identificadores de dispositivos o etiquetas (en la medida en que no se consideren datos personales en algunos países); ii) con tu permiso explícito (por ejemplo, mediante el formulario de generación de contactos); o iii) datos que ya sean visibles para cualquier usuario de los Servicios (por ejemplo, los datos del perfil). Sin embargo, si ves o haces clic en un anuncio dentro o fuera de nuestro sitio web o aplicaciones, el anunciante recibirá una señal de que alguien ha visitado la página que muestra el anuncio y es posible que determinen que has sido tú mediante el uso de mecanismos como las *cookies*. Nuestros socios publicitarios pueden asociar datos personales recopilados por el anunciante directamente de ti con nuestras *cookies* y tecnologías similares. En esos casos, exigimos contractualmente que esos socios publicitarios obtengan tu consentimiento explícito antes de hacerlo.

Como caso particular resalta el de Cívico, quien además de las anteriores finalidades de tratamiento incluye también la

> … configuración de *una base de datos que pueda ser objeto de comercialización,* consulta, transmisión o transferencia de los datos personales a centrales de riesgo y a otras bases de datos de distinta naturaleza, de propiedad de, o administradas por, Cívico

> o por terceros con quienes Cívico tenga relaciones comerciales, contractuales u operativas, con el objeto de que se puedan ofrecer y promover productos y servicios por parte de Cívico o de nuestros socios, terceros y aliados comerciales. Estos terceros destinatarios de las bases de datos y de los datos personales pueden estar ubicados en Colombia o en el exterior. (Énfasis agregado)

Del mismo modo, Duety tiene entre sus finalidades de tratamiento la "cesión de bases de datos".

Por su parte, Unilever incluye entre sus finalidades de tratamiento la de *tomar decisiones automatizadas,* entendidas como aquellas que se toman únicamente por medios automáticos, donde no hay seres humanos involucrados en el proceso de toma de decisiones relacionadas con los datos personales. Según su política de privacidad, claramente influenciada por lo que exige el GDPR,

> … *no tomaremos decisiones basadas únicamente en la toma de decisiones automatizada que tengan un impacto significativo en usted.* Si lo hacemos, se lo haremos saber y le proporcionaremos información clara sobre nuestra decisión de confiar en el tratamiento automatizado para tomar nuestra decisión y nuestra base legal para hacerlo. Usted tiene derecho a no someterse a una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos en usted o le afecte significativamente de modo similar. En particular, usted tiene derecho a: i) obtener intervención humana; ii) expresar su punto de vista; iii) recibir una explicación de la decisión tomada después de una evaluación; iv) impugnar la decisión. (Énfasis agregado)

Relación con Google, Apple, Facebook, Amazon y Microsoft (Gafam)

La relación de las EMNBD con las Gafam es esencialmente de cuatro tipos: i) la aplicación o página web de la empresa permite comenzar sesión a través del inicio de sesión de algún tercero o red social (incluido Facebook, pero no limitado a este); ii) usa botones sociales en su página o aplicación, los cuales son proporcionados por Twitter, Google+, LinkedIn, o Facebook; iii) utiliza Google Analytics, un servicio de Google que usa *cookies* y otras tecnologías de recopilación de datos para reunir información sobre el uso que hacen los usuarios del sitio web y los servicios con

el objetivo de informar acerca de las tendencias de sitios web; iv) dentro de sus socios publicitarios se encuentran compañías que hacen parte del grupo de Google. Mientras la primera relación permite que los Gafam le proporcionen datos personales a las EMNBD, el resto de las relaciones habilitan a los Gafam a acceder a información en poder de estas últimas. Por ejemplo, en el caso de AliExpress se señala que "si se está registrando a una cuenta de AliExpress a través de plataformas de redes sociales como Facebook o Twitter, podemos recopilar el nombre de su cuenta y la foto de perfil en esas plataformas".

Por su parte, resulta interesante el caso particular de 1DOC3, quien se unió a la *iniciativa Internet.org* de Facebook para brindar servicios de internet asequibles en los países menos desarrollados. Además, cabe destacar que ninguna de las empresas que hacen parte de la categoría "empresas establecidas" parece tener relación con los Gafam. Al menos, no más allá de contar con perfiles en sus diferentes páginas.

Por último, es preciso destacar que hay productos (como WhatsApp, YouTube o LinkedIn) que si bien por el nombre no parecen pertenecer a los Gafam, hacen parte de sus grupos empresariales y, en esa medida, comparten información con ellos permanentemente. Por ejemplo, en el caso de WhatsApp su política de privacidad señala: "WhatsApp recibe información de las empresas de Facebook y también comparte información con ellas. Ambas partes podemos usar la información que recibimos para operar, proporcionar, mejorar, entender, personalizar, respaldar y comercializar nuestros servicios y lo que ofrecen".

Como se ve, varias de las fuentes de datos, tratamientos, finalidades y relaciones desarrolladas por las EMNBD aquí estudiadas despiertan preocupaciones similares a las aducidas en su momento por el Grupo de Trabajo del Artículo 29 y citadas más arriba. Entre otras cosas, el surgimiento de las *cookies* como herramienta principal de recolección de datos plantea interrogantes sobre la *gran escala de recopilación de datos y seguimiento* a la que están llegando estas empresas. Lo anterior teniendo en cuenta que las distintas funcionalidades de las *cookies* aquí identificadas muestran la variedad y el detalle de los datos que se pueden llegar a recoger al utilizarlas. Por su parte, la gran variedad de fuentes de datos a las que tienen acceso estas empresas genera interrogantes sobre *las innumerables posibilidades de combinación de datos* con las que cuentan. Asimismo, las relaciones de intercambio de información que se están dando entre los distintos grupos empresariales, así como entre los Gafam y los demás EMNBD, generan

cuestionamientos sobre *la seguridad de los datos que se recolectan*. Esto, partiendo de la base de que las políticas de privacidad le dan al usuario/cliente certeza sobre los sistemas de seguridad utilizados por el respectivo producto, mas no por los productos o las empresas con los que se compartirá esa información, y quienes no parecen tener ningún tipo de compromiso con el titular de los datos. Por su parte, la poca información disponible en relación con los métodos de análisis de datos utilizados por las EMNBD, y, en particular, sobre los algoritmos usados despierta inquietudes sobre *los estándares de transparencia* que se les están exigiendo a estas empresas. Finalmente, la creciente construcción de perfiles (*profiling*) para la provisión de contenidos personalizados y, en ciertos casos, para la toma de decisiones automatizadas, genera riesgos evidentes *para el derecho a la igualdad y la no discriminación de los titulares de los datos.*

Así, animadas por estas preocupaciones comunes, y con la misma aspiración de la Unión Europea de que en el marco de la era digital se logre balancear la innovación y el desarrollo económico con la protección de los derechos y los valores de una sociedad democrática, a continuación pasamos a evaluar el nivel de preparación de nuestro régimen jurídico y de nuestras autoridades competentes para abordar estas nuevas dinámicas propias de la era digital, llamar a rendir cuentas a las EMNBD y prevenir los riesgos descritos.

NIVEL DE PREPARACIÓN DEL RÉGIMEN ACTUAL DE PROTECCIÓN DE DATOS PERSONALES COLOMBIANO Y DE LAS AUTORIDADES COMPETENTES PARA LA ERA DIGITAL

A la luz de la forma de operar de las empresas aquí estudiadas, pasamos ahora a establecer el nivel de "alistamiento" del régimen legal colombiano y de las autoridades competentes para enfrentar los riesgos antes expuestos, y llamar a estas empresas a rendir cuentas en cuanto al tratamiento de datos personales recolectados en Colombia.

Alcance del régimen de protección de datos

En Colombia, el régimen de protección de datos personales se encuentra establecido tanto en el artículo 15 de la Constitución Política (CP) como en dos leyes estatutarias. Por un lado, el artículo 15 CP establece, en su parte pertinente:

> Artículo 15. Todas las personas […] tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

En desarrollo de esa disposición constitucional, y con base en el amplio desarrollo jurisprudencial en la materia, se expidió la Ley Estatutaria 1266 de 2008, que regula el derecho a la protección de datos personales frente a información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Así, dado el carácter sectorial de esta primera ley, tiempo después se expediría la Ley 1581 de 2012 que, a diferencia de la primera, regula de manera general el tratamiento de datos personales en Colombia.

Las disposiciones de esta ley general incluyen los principios de tratamiento de datos personales, a saber: principios de finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Además, disponen los derechos de los titulares de datos personales, los procedimientos para hacer exigible esos derechos, y los deberes de los responsables y encargados del tratamiento. En esta ley también se regulan las condiciones de legalidad del tratamiento de datos personales, y en forma especial, el tratamiento de los datos sensibles y de los datos de los niños, niñas y adolescentes, como categorías especiales. Finalmente, en la Ley 1581 de 2012 también se establecen los mecanismos de vigilancia y sanción del cumplimiento de la ley.

Sin embargo, a partir del estudio detallado del contenido de esta ley general, y de las conductas arriba descritas, se constata que existen varios temas –propios de la era digital– que no son considerados por la legislación actualmente aplicable en Colombia. En particular, en lo que tiene que ver con: i) datos sensibles inferidos, ii) datos vinculados al IP, iii) uso de *cookies*, iv) *web crawling*, v) comercialización de datos, vi) contenidos personalizados, y vii) decisiones automatizadas. De la misma manera, si bien el régimen actual colombiano contempla el uso de los datos para hacer investigaciones académicas, es evidente que las condiciones de regulación de dicha conducta no fueron establecidas para la era digital. De hecho, lo mismo sucede con las condiciones que la ley actual le exige al consentimiento libre, previo e informado del titular para considerarlo válido, las cuales resultan hoy inocuas.

El problema de la inexistente o deficiente regulación sobre temas propios de la era digital radica en la consecuente desprotección de los titulares de los datos personales que sean tratados bajo esas nuevas dinámicas. Lo anterior, teniendo en cuenta el principio de legalidad según el cual, en el caso de los particulares, todo lo que no esté expresamente prohibido, está permitido. Siendo así, al no existir regulación alguna en la materia, se entiende que las fuentes de datos, tratamientos y finalidades que se han popularizado a raíz de la era digital se encuentran en principio permitidas y sin limitación alguna.

A continuación, pasamos a abordar con mayor detenimiento tanto los temas que no están regulados en el régimen colombiano, como aquellos que si bien lo están, requieren de una revisión para garantizar en una mayor medida los derechos a la intimidad, a la protección de datos personales, a la igualdad y no discriminación, y a las libertades relacionadas

(de expresión, de asociación, de libre desarrollo de la personalidad, entre otras) de los titulares de datos.

Lo que no está regulado y debe regularse

Datos sensibles inferidos y los datos de los que se infieren

En Colombia, el concepto de "datos sensibles" se encuentra definido en el artículo 5 de la Ley 1581 de 2012. Según dicho artículo,

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

Como se ve, el concepto no establece, *per se*, que los datos sensibles sean solo aquellos entregados por el titular o por una fuente.[1] En esa medida, bien podría ser un dato sensible aquel que, al ser inferido de otros datos, pueda *revelar* la religión, salud u otras categorías especiales de información del usuario. Y en esa medida, el tratamiento de dicho dato inferido, al igual que el de los demás datos sensibles, estaría prohibido, salvo por las excepciones que plantea el artículo 6 de la Ley 1581, siendo estas: i) que el titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; ii) que el tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado, caso en el cual los representantes legales deberán otorgar su autorización; iii) que el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política,

---

1 Al respecto, es pertinente traer a colación el estudio *Personal Data: The Emergence of a New Asset Class*, publicado por el Foro Económico Mundial en 2011, y en el que se deja claro que el concepto de dato personal incluye no solo los datos "voluntariamente" entregados por el titular, sino también: i) los *datos observados*, que corresponden a aquellos capturados mediante el monitoreo de las acciones de los titulares; y, ii) los *datos inferidos*, correspondientes a aquellos obtenidos a partir del análisis de los datos voluntarios y de los observados (World Economic Forum, 2011).

filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad; y siempre y cuando los datos no sean suministrados a terceros sin la autorización del titular; iv) que el tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; o, v) que el tratamiento tenga una finalidad histórica, estadística o científica, siempre que se adopten las medidas conducentes a la supresión de identidad de los titulares.

Sin embargo, ¿qué sucede con los datos no sensibles (v. gr. las compras hechas en Amazon.com), *que en conjunto con otros* permiten inferir datos sensibles (v. gr. la etnia o la orientación sexual de una persona)? En nuestra opinión, estos datos también deberían ser considerados sensibles, pues finalmente "revelan información que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación".

Al respecto es relevante traer a colación el caso del CCPA de California, en el que si bien no se hace referencia explícita a los datos inferidos sensibles, al menos sí se reconoce explícitamente que los datos inferidos entran dentro del concepto de dato personal. Al respecto, en el literal (o) de la sección 1798.140 se establece que la información personal incluye, entre otras cosas,

> … (K) Inferencias extraídas de cualquiera de la información identificada en esta subdivisión para crear un perfil sobre un consumidor que refleje las preferencias, características, tendencias psicológicas, predisposiciones, comportamiento, actitudes, inteligencia, habilidades y aptitudes del consumidor, los identificadores personales de un consumidor, los datos biométricos, los datos psicométricos, la geolocalización y el historial de navegación por Internet.

La consecuencia práctica de este avance legislativo radica en que, al ser considerados datos personales, las inferencias que se hagan sobre una persona deben estar sujetas a las garantías propias del derecho a la protección de datos, como puede ser, por ejemplo, la necesidad de solicitar autorización del titular del dato para poder realizar cualquier tratamiento sobre él, e informar sobre la finalidad de dicho tratamiento.

Sin embargo, en el caso de Colombia, tanto la definición actual de dato personal como la de dato sensible comprendidas en la legislación parecen no contemplar expresamente esa situación. Lo anterior, pues dicha legislación fue formulada en un momento de desarrollo tecnológico

distinto, en el que no se vislumbraba que los datos personales permitirían, o al menos no con la precisión con la que lo hacen hoy en día por medio de la analítica de datos, inferir nueva información de su titular. En esa medida, en la actualidad podría entenderse que esos datos podrían ser tratados con mayor libertad que los datos sensibles, a pesar de los riesgos que su tratamiento puede generar sobre la intimidad y el derecho a la igualdad de sus titulares.

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

En Colombia, el literal c) del artículo 3° de la Ley 1581 de 2012 define dato personal como "cualquier información *vinculada o que pueda asociarse a* una o varias *personas naturales determinadas o determinables*" (énfasis agregado). Siendo así, la pregunta que surge es: ¿están las direcciones de protocolo de internet (IP) e identificadores similares vinculados o pueden vincularse a una o varias personas naturales determinadas o determinables?

En el caso de la Unión Europea, en el considerando 30 del GDPR se establece que:

> *Las personas físicas pueden ser asociadas a identificadores en línea* facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, *como direcciones de los protocolos de internet*, identificadores de sesión en forma de "cookies" u otros identificadores, como etiquetas de identificación por radiofrecuencia. *Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.* (Énfasis agregado)

Por su parte, el numeral 1° del artículo 4° del GDPR define dato personal como

> … toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un *identificador*, como por ejemplo un nombre, un número de identificación, datos de localización, un *identificador en línea* o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. (Énfasis agregado)

Así, la regulación europea considera que el identificador en línea (*online identifier*) –dentro del cual se encuentran las direcciones IP– permite

determinar, directa o indirectamente (al ser *combinado* con identificadores únicos y otros datos recibidos por los servidores), la identidad de una persona física.

Incluso, desde antes de la expedición del GDPR, y en vigencia de la Directiva 95/46/CE, el Grupo de Trabajo del Artículo 29 ya había considerado las direcciones IP como datos relacionados con una persona identificable. Al respecto, en el documento de trabajo "Privacidad en Internet - Un enfoque integrado de la UE para la protección de datos en línea", expedido el 21 de noviembre de 2000, el Grupo de Trabajo declaró que

> … los proveedores de acceso a internet y los gerentes de redes de área local pueden, usando medios razonables, identificar a los usuarios de internet a quienes les han atribuido direcciones IP, ya que normalmente "registran" sistemáticamente en un archivo la fecha, hora, duración y dirección IP dinámica entregada al usuario de internet. Lo mismo puede decirse acerca de los proveedores de servicios de internet que mantienen un libro de registro sobre el servidor HTTP. En estos casos, *no hay duda sobre el hecho de que uno puede hablar de datos personales en el sentido del Artículo 2 a) de la Directiva.*[2] (Énfasis agregado)

Entonces, dado que en otras latitudes ya parece claro que las direcciones IP permiten identificar de manera directa o indirecta a una persona, a partir del contenido del literal c) del artículo 3° de la Ley 1581 de 2012 se podría interpretar que las mismas están vinculadas a una persona determinable y, en esa medida, se encontrarían incluidas dentro del concepto de dato personal. En consecuencia, lo establecido en la Ley 1581 de 2013 le sería aplicable al tratamiento de dichos identificadores.

Sin embargo, hay ordenamientos jurídicos, como el de California, que plantean aún más certeza al respecto. Así, en el caso del CCPA de California el concepto de "información personal" se ha definido especialmente para incluir, además de los datos biométricos, datos psicométricos, datos de geolocalización y el historial de navegación por internet, identificadores tales como nombre real, alias, dirección postal, identificador personal único, identificadores en línea (dirección IP), dirección de correo electrónico, nombre de cuenta, número de seguro social, número de

2 Grupo de Trabajo del Artículo 29. Documento de trabajo "Privacidad en Internet - Un enfoque integrado de la UE para la protección de datos en línea", noviembre 21 de 2000, 5063/00/EN/FINAL WP 37.

licencia de conducir, número de pasaporte u otros identificadores similares.[3] Una disposición legal de ese tipo permite contar con mucha más certeza jurídica para sostener que las direcciones IP deben ser tratadas bajo las reglas que regulan al resto de los datos personales.

¿Y qué sucede con los datos asociados a esos identificadores? ¿Deberían ser también considerados como datos personales? Piénsese por ejemplo en las búsquedas en Google Search, o en la consulta de artículos en la página web de Almacenes Éxito, cuando aunque el usuario no ha iniciado sesión, su "rastro digital", que ha sido guardado por medio de las llamadas *cookies*, queda asociado con su IP. En nuestra opinión, se trata de información que si bien no está aún vinculada, *podría vincularse a personas determinables.* Lo anterior, pues por medio de los identificadores en línea puede ser asociada a personas determinables; en esta medida, también debería entrar bajo el concepto de dato personal que trae la legislación nacional, y, en consecuencia, ser cubierta por esta.

Sin embargo, hasta que en Colombia no se diga expresamente en la ley, o se interprete por un juez o incluso se proponga como guía por la autoridad reguladora[4] que las direcciones IP son un dato personal y que la información asociada a ellas también lo es, quedaría al arbitrio de cada EMBD determinar si las tratan o no como datos personales. Bajo ese escenario, serán de utilidad relativa cláusulas como la establecida por Apple quien, como ya vimos, menciona que las direcciones IP y los identificadores similares se tratarán como información personal "cuando estos sean así considerados en la legislación local". Del mismo modo, la ausencia de regulación expresa hace que en casos como el de LinkedIn, se le permita

3 Ver literal (o) de la sección 1798.140 del CCPA.

4 En lo que respecta a las posiciones que pueda tomar la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, en su calidad de autoridad de protección de datos, se debe recordar que "los conceptos emitidos por las entidades en respuesta a un derecho de petición de consulta no constituyen interpretaciones autorizadas de la ley o de un acto administrativo. No pueden reemplazar un acto administrativo. Dada la naturaleza misma de los conceptos, ellos se equiparan a opiniones, a consejos, a pautas de acción, a puntos de vista, a recomendaciones que emite la administración pero que dejan al administrado en libertad para seguirlos o no" (Corte Constitucional, Sentencia C-542 de 2015, M. P. Humberto Antonio Sierra Porto). En esa medida, si bien sus posiciones no tienen la misma fuerza ni carácter vinculante que los del legislador o los de la Corte Constitucional, pueden servir como guía para las EMNBD y para las autoridades, al momento de aplicar la ley.

compartir el IP de los usuarios con los anunciantes, pues, como se vio más arriba, esta plataforma no comparte datos personales de sus usuarios con ningún anunciante ni con redes publicitarias para su publicidad "excepto: (i) identificadores de dispositivos o etiquetas (en la medida en que no se consideren datos personales en algunos países)".

Uso de cookies

De acuerdo con nuestra propia Autoridad de Protección de Datos, "en Colombia no existe una regulación específica sobre el uso de *cookies*" (Superintendencia de Industria y Comercio, 2016b). De manera general, el literal g) del artículo 3° de la Ley 1581 de 2012 incluye la recolección como una de las operaciones que constituyen tratamiento de datos personales. De esta manera, a la recolección le son aplicables las obligaciones y garantías establecidas en dicha ley. Sin embargo, la ley no establece nada sobre las herramientas que se utilicen para dicha recolección.

En esa medida, y a partir del principio de legalidad arriba comentado, se entiende que cualquier tipo de herramienta que no contraríe la constitución o la ley puede ser utilizada para recolectar datos, incluidas las *cookies*. Además, eso implica que todo tipo de *cookies* pueden ser implementadas, sin importar si son de sesión, permanentes, propias, de terceros, esenciales para el funcionamiento de la plataforma o la aplicación, para publicidad personalizada o para hacer análisis de sitios web.

Sin embargo, dado que las *cookies* son utilizadas para tratar datos, de acuerdo con el principio de libertad[5] se entiende que la ley actual sí les exige que se obtenga el consentimiento previo e informado del titular de los datos antes de empezar con la recolección de los mismos. En forma similar, en la Unión Europea el numeral 3 del artículo 5º de la Directiva 2002/58/EC (en adelante Directiva E-Privacy), sustituido por el artículo 2º de la Directiva 2009/136/CE, establece que:

> Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, *a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE.* Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica *al solo fin de efectuar la transmisión de una comu-*

5 Ver literal c) del artículo 4 de la Ley 1581 de 2012.

> *nicación a través de una red de comunicaciones electrónicas*, o en la medida de *lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario.*

Así, la Directiva E-Privacy establece expresamente la necesidad de solicitar el consentimiento previo e informado del titular de los datos para instalar *cookies* en su dispositivo y para acceder a la información en ellas almacenada. Sin embargo, y a diferencia de Colombia, la regulación europea en la materia va mucho más allá de la exigencia genérica de un consentimiento previo e informado. Para demostrarlo, es necesario traer a colación varias Opiniones del Grupo de Trabajo del Artículo 29, que si bien no son jurídicamente vinculantes, tienen un importante valor doctrinal al ser proferidas por el organismo consultivo independiente de la Unión Europea en materia de protección de datos y privacidad.

En primer lugar, y tal como se evidencia en la cita arriba transcrita, en la Unión Europea se incluyen excepciones razonables para el consentimiento en el caso de ciertas *cookies*. Al respecto, en la Opinión 4/2012 el Grupo de Trabajo del Artículo 29 señaló de manera expresa que para eximir a una determinada *cookie* del consentimiento previo e informado del titular de los datos era necesario identificar claramente el carácter *sine qua non* de las *cookies* para llevar a cabo: i) la transmisión de comunicaciones en una red de comunicaciones electrónicas; o, ii) la prestación de una funcionalidad explícitamente pedida por el usuario. En otras palabras, se eximen de consentimiento las *cookies* que tienen el carácter de ser condición sin la cual no es posible efectuar una comunicación electrónica o prestar la funcionalidad solicitada por el usuario. Así, se podría decir que son las llamadas *cookies esenciales* las que se encuentran exceptuadas de solicitar el consentimiento del titular de los datos. Sin embargo, el Grupo de Trabajo ha sido claro en que dicha esencialidad debe ser medida desde el punto de vista del usuario, y no del proveedor del servicio (para quien una determinada *cookie* de publicidad comportamental podría ser "esencial" en su estrategia de mercadeo).[6]

Además, y a pesar de que aún no existe regulación al respecto, en la Opinión 4/2012 el Grupo de Trabajo del Artículo 29 también señaló que

---

6 Grupo de trabajo del Artículo 29. *Opinión 4/2012 sobre exención de consentimiento para cookies.* Adoptada en junio 7 de 2012, 00879/12/EN WP 194.

es necesario crear una tercera excepción al consentimiento cuando se trate de *cookies* que están estrictamente limitadas a propósitos estadísticos anonimizados y agregados del responsable de la página web. Es decir, cuando se trate de *cookies* para hacer análisis de sitios web que recolecten información de manera anonimizada y agregada.[7] Frente al particular, cabe notar que la Directiva E-Privacy está bajo reforma desde enero de 2017, cuando el Consejo de la Unión Europea publicó su propuesta para mejorar y actualizar sus garantías (European Commission, 2017).

En segundo lugar, la regulación europea es incluso más estricta en lo que se refiere al consentimiento de las *cookies* para publicidad comportamental.[8] Así, en la Opinión 2/2010 el Grupo de Trabajo del Artículo 29 dejó sentado que en el caso de esa clase de *cookies* dicha solicitud de consentimiento debe informar: i) quién es el responsable de instalar la *cookie* y de recolectar la información allí guardada; ii) que la *cookie* será utilizada para crear perfiles; iii) qué tipo de información será recolectada para construir esos perfiles; iv) que los perfiles serán utilizados para entregarle publicidad dirigida; v) que la *cookie* permitirá identificar al usuario en múltiples sitios web.[9]

Evidentemente, el desarrollo del contenido del consentimiento de este tipo de herramientas digitales, así como de sus excepciones, brilla por su ausencia en el régimen de protección de datos personales colombiano. En consecuencia, las políticas de privacidad aquí estudiadas no se ven obligadas a contar con una descripción detallada sobre las finalidades publicitarias y de *profiling* que tiene la recolección de los datos. De igual forma, suelen incluir en la misma autorización el uso de *cookies* esenciales y las que no lo son, y advierten que su rechazo puede acarrear la imposibilidad de acceder a algunas de las funcionalidades de una determinada plataforma. Por último, la ausencia de regulación en la materia hace que

---

7 *Idem.*

8 De acuerdo con el Grupo de Trabajo del Artículo 29, la publicidad comportamental es aquella "publicidad que se basa en la observación del comportamiento de las personas a lo largo del tiempo. La publicidad comportamental busca estudiar las características de este comportamiento a través de sus acciones (visitas repetidas al sitio, interacciones, palabras clave, producción de contenido en línea, etc.) para desarrollar un perfil específico y proporcionarles a los interesados una publicidad adaptada a sus intereses" (Grupo de trabajo del Artículo 29. *Opinión 2/2010 sobre publicidad comportamental en línea.* Adoptada en junio 22 de 2010, 00909/10/EN WP 171, 4).

9 *Idem*.

se termine pidiendo consentimiento del titular incluso en los casos en los que las *cookies* son utilizadas para: i) la captura de información necesaria para realizar el propósito por el cual la persona acude a los servicios de la EMNBD, ya sea para optimizar la navegación en su sitio web, para poder celebrar un contrato (comprar un tiquete aéreo, realizar un pago) o para registrarse en y hacer uso de una plataforma (red social o suscripción); y, ii) la captura de información anonimizada o agregada para propósitos exclusivamente estadísticos del responsable de la página web.

El web crawling

Como ya vimos, el *web crawling* consiste en la utilización de programas informáticos que navegan la web e indexan contenidos. Si bien el *web crawling* no apareció como una de las fuentes de datos más usadas por las EMNBD aquí estudiadas, su utilización, en casos como el de la plataforma Google Search, plantea interrogantes importantes en el marco de la protección de datos personales. Lo anterior, en la medida en que nos lleva a preguntarnos si la indexación de contenidos implica algún tipo de tratamiento de datos personales, o si, por el contrario, se trata del cumplimiento de un simple rol de intermediario entre los proveedores de contenidos (que tienen a su vez la categoría de responsables del tratamiento de los datos personales allí incluidos) y los usuarios de contenidos (que tienen la categoría de usuarios[10] o destinatarios de datos personales). En otras palabras, el uso del *web crawling* por parte de algunas EMNBD nos hace preguntarnos si los gestores de motores de búsqueda, como Google Search o Yahoo! Search, al indexar contenidos, pueden ser considerados responsables del tratamiento de datos personales, y, en esa medida, deben: i) garantizar los derechos al acceso, rectificación, actualización o supresión que tienen los titulares de los datos por ellos tratados; ii) cumplir con las obligaciones relativas a la calidad y la actualización de los datos, a la solicitud de autorización del titular, entre otras.

---

10 De acuerdo con el literal d) del artículo 3° de la Ley 1266 de 2018, "el usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos".

En el caso de Europa, dicho interrogante fue resuelto por el Tribunal de Justicia de la Unión Europea en la sentencia del caso Google Spain, S.L., y Google Inc., *vs.* Agencia Española de Protección de Datos y Costeja González, fallada el 13 de mayo de 2014. En esa ocasión se discutía si la Agencia Española de Protección de Datos había actuado en derecho al ordenar a Google Inc. que adoptara las medidas necesarias para retirar los datos personales del Sr. Costeja González de su índice e imposibilitara el acceso futuro a la publicación del periódico *La Varguardia*, que los contenía. Para resolver dicha cuestión, y de forma similar a lo aquí planteado, el Tribunal de Justicia se preguntó:

> … en relación con la actividad [de Google Search], como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos", contenido en el art. 2.b de la [Directiva 95/46]?

Al respecto, se consideró que

> … un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o solo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo (véase, en este sentido, la Sentencia eDate Advertising y otros, C-509/09 y C-161/10, EU:C:2011:685, apartado 45).

En consecuencia, se concluyó que

> … por un lado, la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, *debe calificarse de "tratamiento de datos personales"*, en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro, *el gestor de un motor de búsqueda debe considerarse "responsable" de dicho tratamiento*, en el sentido del mencionado artículo 2, letra d). (Énfasis agregado)

A raíz de esa sentencia quedó sentado que en el caso de la Unión Europea, los titulares de los datos tratados mediante *web crawling* pueden exigir a los intermediarios de internet, entre otras cosas, que por medio de la desindexación supriman los resultados obtenidos luego de utilizar descriptores correspondientes a datos personales.

En contraste, en el caso de Colombia la posición jurisprudencial ha sido distinta. Dado que la legislación no dice nada sobre la materia, la Corte Constitucional tuvo que resolver este interrogante en la Sentencia T-040 de 2013. En esa sentencia la Corte analizaba si la Casa Editorial El Tiempo S.A., y Google Colombia Ltda. habían vulnerado los derechos fundamentales al buen nombre, honra y dignidad humana del señor Guillermo Martínez Trujillo, al no eliminar de sus archivos y registros el artículo denominado "Los hombres de la mafia de los Llanos", en el cual se nombraba al accionante como integrante de un cartel de estupefacientes. A diferencia del caso *Costeja*, en Colombia la Corte terminó por tutelar los derechos del accionante y ordenar a la Casa Editorial El Tiempo, y no al motor de búsqueda, que procediera a modificar tanto el título como el contenido de la noticia. Por su parte, frente a la responsabilidad del buscador de internet señaló lo siguiente, que por su importancia se transcribe *in extenso*:

> Finalmente, advierte la Sala que en el caso concreto, el responsable de la información emitida, y por ende de su posible rectificación, es el medio de comunicación que recolectó, analizó, procesó y divulgó la noticia, es decir, la casa Editorial El Tiempo, a través de su página electrónica oficial. En ese orden a quien procede realizar la rectificación, en caso dado, es a esta entidad. Por el contrario, para la Sala de Revisión, Google Colombia S.A. no es responsable de la noticia "Los hombres de la mafia de los

> Llanos", pues como bien lo explicó esta empresa en el escrito de contestación, *Google presta un servicio de búsqueda de la información que hay en toda la red, y no es quien redacta o publica tal información, sino que es un simple motor de búsqueda al cual no se le puede endilgar la responsabilidad sobre la veracidad o imparcialidad de un respectivo artículo, noticia o columna que aparezca en sus resultados.*
>
> *Señaló el representante de Google Colombia acertadamente que "el proveedor de servicios de búsquedas, no es responsable del contenido de las páginas que figuren como resultados de búsquedas*, ni tampoco es responsable como erróneamente lo afirma el accionante por 'mantener en sus registros' determinada información". Referente a lo anterior, Google administra un índice que vincula palabras con direcciones URL de páginas de internet, es decir, "es el fichero de una gran biblioteca que es internet y como tal, por su intermedio se ordenan las páginas de internet que, siguiendo con el ejemplo dado, serían los libros de esa supuesta biblioteca". La información que es ingresada a internet por los dueños de las páginas de internet determina cuál es el resultado que los usuarios de Google recibirán como respuesta a sus búsquedas que abarcan temas complejos o intereses concretos de cada persona. En virtud de ello, por los elementos fácticos y para efectos de resolver el caso *sub examine, no es competencia ni responsabilidad de Google, rectificar, corregir, eliminar o complementar la información que arroja una búsqueda concreta, sino del medio de comunicación, escritor, columnista, etc., que incluye y procesa la información en internet. Sin perjuicio de que, por características distintas, haya casos donde una base de datos que cumple la función de Google, pueda generar alguna vulneración de un derecho fundamental por la información que administra.*[11] (Énfasis agregado)

Tiempo después, y habiéndose ya fallado la sentencia del Tribunal de Justicia de la Unión Europea arriba citada, la Corte Constitucional volvería a abordar este tema en la Sentencia T-277 de 2015, en la que se discutió si la indexación del portal de internet donde se publicó una noticia de la Casa Editorial El Tiempo lesionaba los derechos fundamentales de la titular de los datos personales allí incluidos, la señora "Gloria". En esa ocasión, la Corte consideró que

---

11 Corte Constitucional, Sentencia T-040 de 2013, M. P. Jorge Ignacio Pretelt Chaljub.

> … una solución como la adoptada por el Tribunal de Justicia de la Unión Europea en el caso Costeja v. AEPD, si bien representa un mecanismo de garantía del derecho al buen nombre de la persona afectada por la difusión de la noticia, implica a la vez un sacrificio innecesario del principio de neutralidad de Internet y, con ello, de las libertades de expresión e información.[12]

En contraste, determinó que

> … *la vulneración del derecho fundamental no es imputable en este caso a Google en tanto no es responsable de producir la información.* Adicionalmente, estima necesario señalar que la razón para no acceder a la desindexación consiste en la protección del principio de neutralidad de la red que, como ya se mencionó, solo puede ser restringida en situaciones excepcionales, ya citadas previamente.[13]

En esa medida, y de manera alternativa al Tribunal de Justicia de la Unión Europea, se optó por ordenarle al periódico *El Tiempo*, en su calidad de proveedor del contenido disputado, que por medio del uso de herramientas técnicas como "robots.txt" y "metatags", impidiera que el contenido específico fuera mostrado como resultados al realizar una consulta por medio de un buscador de internet.

Frente a estos dos pronunciamientos judiciales nacionales es preciso destacar tres cosas. En primer lugar, es interesante resaltar que si bien en ninguna de las dos sentencias se declaró la responsabilidad del buscador, en la primera se dejó abierta la posibilidad de futuras responsabilidades. Lo anterior, a partir de la expresión:

> … no es competencia ni responsabilidad de Google, rectificar, corregir, eliminar o complementar la información que arroja una búsqueda concreta, sino del medio de comunicación, escritor, columnista, etc., que incluye y procesa la información en internet. *Sin perjuicio de que, por características distintas, haya casos donde una base de datos que cumple la función de Google, pueda generar alguna vulneración de un derecho fundamental por la información que administra.*[14] (Énfasis agregado).

---

12 Corte Constitucional, Sentencia T-277 de 2015, M. P. María Victoria Calle Correa.

13 *Idem.*

14 Corte Constitucional, Sentencia T-040 de 2013, M. P. Jorge Ignacio Pretelt Chaljub.

En segundo lugar, llama la atención que si bien en ambas sentencias se señala al medio de comunicación como el responsable de la violación de derechos, las órdenes adoptadas por la Corte son muy distintas. Así, mientras en el caso "Los hombres de la mafia de los Llanos" se ordenó la modificación del artículo periodístico, en el caso de la señora "Gloria" se optó por ordenar la utilización de determinadas herramientas tecnológicas para "des-taggear" el contenido objeto de disputa y que el buscador no lo pudiera encontrar.

Finalmente, es importante resaltar que en las dos sentencias citadas la Corte consideró que, dado que se trataba de información periodística, el derecho en juego no era el de protección de datos personales,[15] sino los derechos a la honra y al buen nombre. En esa medida, las decisiones adoptadas, si bien exoneraron de responsabilidad al gestor del motor de búsqueda, no tuvieron en consideración si este estaba o no haciendo tratamiento de datos personales. Este último punto es fundamental pues demuestra que, a diferencia de Europa, en Colombia el carácter de responsables de tratamiento de datos personales de quienes realizan *web crawling* es un asunto que aún continúa por definirse, ya sea por medio de la ley o de un nuevo pronunciamiento de la Corte.

Comercialización de datos

La única disposición legal que en Colombia hace referencia expresa a la comercialización de datos personales se encuentran consagrada en el artículo 269F del Código Penal sobre el delito de violación de datos personales. Según dicho artículo:

> Artículo 269F. Violación de datos personales. 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 de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Énfasis agregado)

---

15 Por ejemplo, en la Sentencia T-040 de 2013 se señaló: "el derecho fundamental de *habeas data* invocado por el actor, no es aplicable al caso, toda vez que la discusión se centra en la información periodística difundida por un medio de comunicación en el ejercicio de la libertad de expresión, y en su rectificación, no de una información de una base de datos o archivos regulada por la Ley Estatutaria analizada por esta Corporación en Sentencia C-748 de 2011" (Corte Constitucional, Sentencia T-040 de 2013, M. P. Jorge Ignacio Pretelt Chaljub).

Dado que el delito consiste, entre otras cosas, en vender datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes *sin estar facultado para ello*, se infiere que en Colombia es legal vender dicha información cuando se está facultado para el efecto. ¿Cuándo se está facultado? Partiendo del principio de libertad[16] propio de la protección de datos personales, suponemos que al igual que el resto de los tratamientos de datos personales, se está facultado para comercializar datos cuando se obtiene el consentimiento previo, expreso e informado del titular de los mismos, o en presencia de mandato legal o judicial que releve de tal consentimiento.

En esa medida, la autorización del titular, o la exigencia de un mandato legal o judicial parecen ser la única limitación que existe en Colombia para llevar a cabo la comercialización de datos. Sin embargo, debe recordarse que en el capítulo 3 de este documento presentamos la comercialización de datos no solo como un tipo de tratamiento, sino también como una finalidad. Entonces, en caso de ser una finalidad, la comercialización de datos –principalmente utilizada para vender información a la industria del *marketing* de datos (*data brokers*)– estaría también condicionada por el principio de finalidad establecido en el literal b) del artículo 4° de la ley en comento. Según dicho principio, "el Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular".

¿Es legítima, según la constitución y la ley colombiana, la comercialización de datos personales? En principio, y con respecto al tratamiento de datos llevado a cabo por empresas privadas, sí lo es. Lo anterior, pues, como se señaló, a los sujetos privados les es aplicable el principio de legalidad según el cual, todo lo que no está prohibido está permitido. Entonces, dado que no existe disposición alguna que prohíba la venta de datos con autorización del titular, esta actividad parece ser legal. Incluso, también parece permitirse la postura –planteada por todas las EMNBD aquí estudiadas–, según la cual los datos hacen parte de los activos de las empresas, y como tales, pueden ser vendidos o cedidos en caso de que se venda o fusione esta última.

Sin embargo, esta incipiente regulación de la comercialización de datos o del *data brokering* contrasta con el CCPA de California, en el que se permite expresamente a los consumidores prohibir la venta de su

16 Ver literal c) del artículo 4 de la Ley 1581 de 2012.

información personal por parte de una empresa (referido en la ley como el derecho a *opt out*), y se le prohíbe a la compañía tomar represalias o discriminar a un consumidor en términos de precio o calidad del bien o servicio ofrecido por ejercer este derecho,[17] "excepto si la diferencia [en el precio o calidad] está razonablemente relacionada con el valor proporcionado al consumidor por sus propios datos".[18] Además, a las empresas se les prohíbe vender la información personal de los consumidores menores de 16 años, a menos 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 a *opt in*).[19]

Pero, además, la incipiente regulación colombiana desestima riesgos evidentes que se derivan de la venta de datos personales. Al respecto, resulta pertinente recordar que según el Grupo de Trabajo del Artículo 29, el *data broker* es aquella empresa que

> … recopila datos de diferentes fuentes públicas y privadas, ya sea en nombre de sus clientes o para sus propios fines. […] compila los datos para desarrollar perfiles de los individuos y los ubica en segmentos. Vende esta información a las empresas que desean mejorar la orientación de sus productos y servicios. […] elabora el perfil colocando a una persona en una determinada categoría de acuerdo con sus intereses.[20]

Esta definición es relevante pues, tal y como lo reconoció la Corte Constitucional de Colombia en la Sentencia T-414 de 1992,

> … el "perfil de datos" de la persona se constituye entonces en una especie de "persona virtual" sobre la cual pueden ejercerse muchas acciones que tendrán repercusión sobre la persona real. Desde el envío de propaganda no solicitada, hasta coerción u "ostracismo" social como en el caso que se presenta. Un "buen" manejo de Bancos de Datos permitiría identificar hasta perfiles poblacionales desde distintos puntos de vista, lo cual constituye un evidente peligro de control social de aquellos que ostentan "poder informático", no solamente contra la libertad de las per-

---

17 Ver literal (a) de la sección 1798.120 del CCPA.

18 Ver numeral (2) del literal (a) de la sección 1798.125 del CCPA.

19 Ver literal (c) de la sección 1798.120 del CCPA.

20 Grupo de Trabajo del Artículo 29. *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptadas en octubre 3 de 2017, 17/EN WP251rev.01, 8.

> sonas individuales sino contra la de sectores sociales más amplios.[21]

En igual sentido, el Grupo de Trabajo del Artículo 29 ha reconocido que la elaboración de perfiles (*profiling*) plantea riesgos para los derechos y las libertades de las personas, en la medida en que

> … estos procesos pueden ser opacos. Las personas pueden no saber que están siendo perfiladas o comprender lo que está involucrado. La creación de perfiles puede perpetuar los estereotipos existentes y la segregación social. También puede bloquear a una persona en una categoría específica y restringirla a sus preferencias sugeridas. Esto puede socavar su libertad de elegir, por ejemplo, ciertos productos o servicios, como libros, música o noticias. En algunos casos, la creación de perfiles puede generar predicciones inexactas. En otros casos, puede conducir a la denegación de servicios y bienes y a una discriminación injustificada.[22]

Ejemplos de la perpetuación de estereotipos existentes y de la segregación social que puede ser generada por el *profiling* se encuentran en casos como el del llamado *big data policing* (Ferguson, 2017), en el que el *profiling* es utilizado por las autoridades de policía para predecir el crimen, con base en determinados perfiles que son construidos a partir de datos cuya neutralidad racial es seriamente cuestionada, y que, en esa medida, pueden perpetuar estereotipos discriminatorios. Otro ejemplo es el uso del *profiling* para predecir el rendimiento y potencial de candidatos a una vacante laboral, cuyos criterios de valoración pueden estar sesgados por datos personales sensibles como el género o el estrato socioeconómico de los aspirantes.

Entonces, si los *data brokers* compran datos personales para elaborar perfiles de los titulares de datos, y es claro que dichos perfiles constituyen un evidente peligro de control social, discriminación y restricción de libertades, no se entiende por qué estos, así como la venta de datos que los hace posibles, pueden ser libremente realizados por las EMNBD que recolectan datos en Colombia, sin que exista regulación específica al respecto.

---

21 Corte Constitucional, Sentencia T-414 de 1992, M. P. Ciro Angarita Barón.

22 Grupo de Trabajo del Artículo 29. *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptadas en octubre 3 de 2017, 17/EN WP251rev.01, 5-6.

En contraste, en el caso de la Unión Europea, por medio del GDPR se ha intentado promover la *transparencia* de la construcción de perfiles. Así en el considerando 60 se estableció: "se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración". Igualmente, dado que el proceso de *profiling* implica la generación de información "nueva" (inferida) que no fue entregada de manera directa por el titular de los datos, el artículo 14 del GDPR impone exigencias particulares de transparencia cuando los datos no fueron provistos "voluntariamente" por el titular. Entre ellas, resulta interesante citar la exigencia de informar al titular de la existencia de esa información en poder del responsable del tratamiento "dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos".[23]

Asimismo, al interpretar el literal a) del numeral 1 del artículo 5 del GDPR para el caso del *profiling*, el Grupo de Trabajo del Artículo 29 ha dicho que "la elaboración de perfiles puede ser injusta y crear discriminación, por ejemplo, al negar a las personas el acceso a oportunidades de empleo, crédito o seguro, o dirigirles productos financieros excesivamente arriesgados o costosos".[24] Por eso, por medio del GDPR también se intentó incentivar el *carácter justo* de los tratamientos de datos, incluido el *profiling*.

Contenidos personalizados

El ofrecimiento de contenidos personalizados (incluidos anuncios y publicidad) es una de las finalidades del tratamiento de datos personales que realizan las EMNBD aquí estudiadas. Sin embargo, el régimen de protección de datos personales actualmente vigente en Colombia no regula nada al respecto, más allá de la exigencia general de que dicha finalidad, al igual que las demás que se puedan tener: i) sea legítima de acuerdo con la Constitución y la Ley, y, ii) sea informada al titular al momento de recoger los datos personales.

Infortunadamente, el limitado alcance de dicha regulación deja de lado muchas particularidades que deben ser tenidas en cuenta a la hora de permitir el uso de los datos personales para el suministro de contenidos,

---

23 Literal a) del numeral 3 del artículo 14 del GDPR.

24 Grupo de Trabajo del Artículo 29. *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptado en octubre 3 de 2017, 17/EN WP251rev.01, 10.

y, en particular, de publicidad personalizada. En primer lugar, pasa por alto que la publicidad personalizada se basa en el *profiling*,[25] práctica que, como vimos, plantea riesgos significativos para los derechos y las libertades de las personas. En segundo lugar, desestima el hecho de que la publicidad personalizada no es siempre igual, pudiendo ser más o menos invasiva de la privacidad de las personas. Así, por un lado, tenemos la *publicidad contextual*, "que se selecciona en función del contenido que está viendo actualmente el titular de los datos".[26] Le sigue la *publicidad segmentada*, que consiste en "publicidad seleccionada con base en las características conocidas del titular de los datos (edad, sexo, ubicación, etc.), que el titular proporcionó en la etapa de inicio de sesión o registro".[27] Finalmente, y con el nivel más invasivo, se encuentra la *publicidad comportamental*, que consiste en

> … publicidad que se basa en la observación del comportamiento de las personas a lo largo del tiempo. La publicidad comportamental busca estudiar las características de este comportamiento a través de sus acciones (visitas repetidas al sitio web, interacciones, palabras clave, producción de contenido en línea, etc.) para desarrollar un perfil específico y proporcionarles a los interesados una publicidad adaptada a sus intereses.[28]

En tercer lugar, la regulación casi inexistente en la materia subestima el hecho de que en la publicidad comportamental está involucrado más de un actor por regular. En esa medida, es probable que en su ejecución no intervengan solo las EMNBD aquí estudiadas, que son quienes teniendo un determinado servicio web proveen espacios publicitarios, sino que también intervienen: i) los anunciantes y ii) los proveedores de redes publicitarias. Así, mientras las EMNBD reservan espacio publicitario en su sitio web para mostrar un anuncio, ceden el resto del proceso publicitario

---

25 Al respecto, cabe destacar que la publicidad dirigida es posible a través de "tecnología básica de Internet [que] permite a los proveedores de redes publicitarias rastrear titulares de datos en diferentes sitios web y en el tiempo. La información recopilada sobre el comportamiento de navegación de los titulares de datos se analiza con el fin de crear perfiles exhaustivos sobre los intereses de los interesados. Dichos perfiles se pueden utilizar para proporcionar a los interesados una publicidad personalizada" (Grupo de trabajo del Artículo 29. *Opinión 2/2010 sobre publicidad comportamental en línea.* Adoptada en junio 22 de 2010, 00909/10/EN WP 171, 4).

26 *Ibid*., 5.

27 *Idem*.

28 *Ibid*., 4.

a uno o más proveedores de redes publicitarias. Estos, por su parte, instalan *cookies* en las páginas web de todos sus clientes, para monitorear a los usuarios y "rastrear" su comportamiento. De esta manera, crean perfiles de los usuarios con base en los cuales pueden recomendarle a los anunciantes en qué espacios publicitarios promover sus productos.[29] Entonces, tal y como ya se ha identificado en la Unión Europea, en ese tipo de publicidad "la proliferación de actores y la complejidad tecnológica de la práctica hacen que sea difícil para el titular saber y entender si, por quién y con qué propósito se recopilan datos personales relacionados con él".[30]

Por eso, se hace necesario que la finalidad de provisión de contenidos personalizados (y en particular de publicidad comportamental) sea expresamente regulada, para evitar tanto la invasión ilegítima de la privacidad de los usuarios/clientes de las EMNBD, como su total ignorancia frente a una actividad, basada en sus datos, de la que están sacando provecho varios actores.

Toma de decisiones automatizadas

La toma de decisiones automatizadas ha sido definida como "la habilidad de tomar decisiones por medios tecnológicos sin intervención humana".[31] De acuerdo con el principio de finalidad que establece la Ley 1581 de 2012, "el Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular". En esa medida, en caso de que la toma de decisiones automatizadas sea una finalidad de tratamiento, se entiende que la misma debe ser: i) legítima de acuerdo con la Constitución y la ley, ii) ser comunicada al titular de los datos. Además, el artículo 5 del Decreto reglamentario de la ley en comento exige que dicha finalidad sea específica.[32] No obstante, y al igual que sucede con la provisión de contenidos personalizados, estos tres condicionamientos dejan por fuera muchos otros requisitos que son fundamentales

---

29 *Idem*.

30 Considerando 58 del GDPR.

31 Grupo de Trabajo del Artículo 29. *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptado en octubre 3 de 2017, 17/EN WP251rev.01, 8.

32 Según el artículo 5 del Decreto 1377 de 2013, "el Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del tratamiento para las cuales se obtiene el consentimiento".

para prevenir que dichas decisiones sin intervención humana pongan en peligro los derechos de los titulares de los datos allí involucrados.

Para el efecto, resulta relevante citar el artículo 22 del GPDR, según el cual:

> Artículo 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles*
>
> 1. Todo 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.*
> 2. El apartado 1 no se aplicará si la decisión:
>
> a) es *necesaria para la celebración o la ejecución de un contrato* entre el interesado y un responsable del tratamiento;
>
> b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
>
> c) se basa en el *consentimiento explícito* del interesado.
>
> 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el *derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.*
> 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Así, a diferencia de Colombia, en la Unión Europea ya han tomado medidas para prevenir los posibles riesgos de las decisiones automatizadas. Por ello, en el GDPR no solo se le dio al titular de los datos la opción de rechazar dicha finalidad de tratamiento si la misma puede producir efectos jurídicos en él[33] o lo afecte significativamente de modo

---

33 Lo que según el Grupo de Trabajo del Artículo 29 implica que afecte derechos legales, como la cancelación de un contrato, el acceso a un determinado beneficio social, o la admisión a un país (Grupo de Trabajo del Artículo 29. *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679*. Adop-

similar.[34] Adicionalmente, en caso de aceptar dicha finalidad, se le otorgaron los derechos a: i) obtener intervención humana por parte del responsable, ii) expresar su punto de vista, iii) impugnar la decisión. Además, se prohibió expresamente la toma de decisiones automatizadas con base en datos sensibles, salvo que sea un tratamiento expresamente autorizado por el titular de los datos, o que sea necesario por razones de interés público, casos en los cuales se deben haber adoptado las debidas salvaguardas.

Estos condicionamientos, si bien aún limitados,[35] le apuntan a *transparentar* el funcionamiento de las decisiones automatizadas, para que el titular de los datos tenga un mayor control sobre las decisiones que se toman sobre él. En esa medida, parecen estar acordes con los Principios Rectores sobre Empresas y Derechos Humanos, que traen consigo medidas en materia de transparencia. En particular, en su recomendación 21 se establece:

> … Para explicar las medidas que toman para hacer frente a las consecuencias de sus actividades sobre los derechos humanos, *las empresas deben estar preparadas para comunicarlas exteriormente, sobre todo cuando los afectados o sus representantes planteen sus inquietudes.* Las empresas cuyas operaciones o contextos operacionales implican graves riesgos de impacto sobre los derechos humanos deberían informar oficialmente de las medidas que toman al respecto. En cualquier caso, las comunicaciones deben reunir las siguientes condiciones: a) Una forma y una frecuencia *que reflejen las consecuencias de las actividades de la empresa sobre los derechos humanos* y que sean accesibles para sus destinatarios; b) Aportar suficiente información para evaluar si la respuesta de una empresa ante consecuencias concretas sobre los derechos humanos es adecuada; c) No poner en riesgo, a su vez, a las partes afectadas o al personal, y no vulnerar requisitos legítimos de confidencialidad comercial.

---

tado en octubre 3 de 2017, 17/EN WP251rev.01).

34 Lo que según el Grupo de Trabajo del Artículo 29 implica que la decisión tenga el potencial de: i) "afectar significativamente las circunstancias, comportamientos o elecciones de las personas involucradas"; ii) "tener un impacto prolongado o permanente en el titular de los datos"; o, iii) "en su forma más extrema, conducir a la exclusión o discriminación de las personas" (Grupo de Trabajo del Artículo 29. *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptado en octubre 3 de 2017, 17/EN WP251rev.01, 21).

35 En particular, aún no es claro qué implica una afectación "significativa", lo cual en la prática puede restarle efectividad a estos condicionamientos.

Del mismo modo, parecen coincidir con lo establecido en la Resolución de las Naciones Unidas sobre el Derecho a la Privacidad en la Era Digital A/C.3/71/L.39, en la que se exhorta a los países y a las empresas a que:

> … i) Consideren medidas apropiadas para que las empresas adopten medidas voluntarias de transparencia para responder a solicitudes arbitrarias o ilegales de las autoridades estatales que requieren acceso a datos e información privada de los usuarios; […] l) Aseguren que las decisiones basadas en un tratamiento automatizado que afecte de manera significativa los derechos de una persona sean transparentes y no tengan efectos discriminatorios.

Lo que está inadecuadamente regulado

Posibilidad de compartir datos personales para investigaciones académicas

Al igual que las políticas de privacidad de las EMNBD aquí estudiadas, el ordenamiento jurídico colombiano contempla expresamente la posibilidad de que el responsable de los datos personales los comparta con terceros para fines de investigación académica (en particular, de carácter histórico, estadístico o científico). De hecho, incluye esa situación como uno de los casos en donde la autorización del titular no es necesaria. Así, el literal d) del artículo 10 de la Ley 1581 de 2012 establece que "la autorización del Titular no será necesaria cuando se trate de: d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos". En el mismo sentido, incluye esa situación como uno de los casos en los que sí está permitido efectuar tratamiento de datos personales sensibles, aunque hace la salvedad de que "en este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares".[36]

En nuestra opinión, la exigencia de anonimizar los datos sensibles resulta insuficiente de cara a la era digital en la que, como se comentó, es tal el volumen de datos que la identidad de su titular podría eventualmente ser reidentificada. De hecho, esa parece se la posición de la Unión Europea, en donde incluso desde antes del GDPR se ha exigido que a la hora de compartir datos personales para investigaciones académicas el responsable de los datos se asegure de que las medidas para anonimizar (y demás *safeguards* que se tomen, como pueden ser la agregación de datos

36 Ver literal e) del artículo 6 de la Ley 1581 de 2012.

o la pseudoanonimización):[37] i) impidan que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona;[38] y, ii) sean acompañadas por un test de compatibilidad (*compatibility assesment*) en el que se analice, en cada caso concreto, si el tratamiento con fines de investigación es compatible con el fin para el cual se recogieron inicialmente los datos personales. Para ello, el Grupo de Trabajo del Artículo 29 estableció cuatro criterios que deberían ser tenidos en cuenta,[39] y que luego serían incluidos en el numeral 4° del artículo 6 del GDPR, a saber: a) cualquier relación entre los *fines* para los cuales se hayan recogido los datos personales y los fines de la investigación; b) el *contexto* en que se hayan recogido dichos datos, en particular en lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la *naturaleza* de los datos personales, en concreto cuando se traten categorías especiales, o aquellos relativos a condenas e infracciones penales; d) las *posibles consecuencias* para los interesados del tratamiento ulterior previsto.

Así, a diferencia de Colombia, en la Unión Europea se ha establecido que solo se podrá proceder con el tratamiento –siempre anonimizado – de datos personales para fines de investigación; cuando se compruebe que los objetos de la investigación se relacionan con los fines iniciales para los que la información fue recolectada; que la relación entre los titulares de los datos y los responsables no es desbalanceada o implicó algún tipo de coacción; que no se trata de categorías especiales de datos personales, y que la correspondiente investigación académica no acarreará consecuencias sobre la vida de los titulares de los datos por tratar.

Evidentemente, se trata de garantías que no pueden deducirse de la normatividad colombiana, y cuya existencia haría que la posibilidad de compartir datos personales sensibles para investigaciones académicas estuviese más limitada, a fin de asegurar la prevalencia de los derechos de los titulares de esos datos, aunque sin entorpecer con ello el avance de la ciencia.

---

37 Definida en el literal 5 del artículo 4 del GDPR como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

38 Ver considerando 29 de la Directiva 95/46/EC.

39 Ver Grupo de Trabajo del Artículo 29. *Opinión 03/2013 sobre la limitación de finalidad.* Adoptado en abril 2 de 2013, 00569/13/EN WP 203.

Consentimiento previo, expreso e informado

Dado que, como vimos, las disposiciones de la Ley 1581 de 2012 no se refieren expresamente a ninguna de las actividades antes mencionadas (comercialización de datos, *profiling*, toma de decisiones automatizadas), las mismas podrán ser realizadas una vez el titular de los datos dé su consentimiento previo, expreso e informado, el cual deberá ser obtenido por cualquier medio que pueda ser objeto de consulta posterior.[40]

En la práctica, en Colombia dicho consentimiento se da aceptando un conjunto de políticas de privacidad (legalmente denominadas "políticas de tratamiento de información") que por ley deben publicar las EMNBD, las cuales: i) por su extensión, pocas personas suelen leer; ii) por su complejidad, pocas personas suelen entender; iii) por su vaguedad, resulta difícil dimensionar las implicaciones de aceptarlas. Además, se trata de políticas que no dan libertad al titular de los datos para seleccionar los tratamientos y las finalidades que desee autorizar, pues: a) presentan la información en bloque, sin que se le permita al titular excluir algunos tratamientos o finalidades y aceptar otros; b) condicionan la prestación del servicio a la aceptación completa de dichas políticas. Incluso, en algunos casos el usuario no tiene que enfrentarse a las mencionadas políticas de privacidad, pues es recurrente que muchas de las EMNBD asuman que la permanencia del usuario en la aplicación o en la plataforma es, como lo dice el Decreto reglamentario de la Ley 1581 de 2012, una "conducta […] inequívoca […] del Titular que permite concluir de forma razonable que otorgó la autorización".[41]

Evidentemente, este diagnóstico pone en duda la utilidad del consentimiento previo, expreso e informado para proteger *efectivamente* el derecho a la protección de datos personales de los titulares de los datos.[42] En

---

40 Ver artículo 9 de la Ley 1581 de 2012.

41 Artículo 7 del Decreto 1377 de 2013. Lastimosamente, al preguntársele a la Superintendencia de Industria y Comercio sobre la legalidad de esta práctica, el jefe de la Oficina Asesora Jurídica respondió: "esta Oficina Asesora Jurídica no es competente para determinar si un titular de los datos personales al utilizar un sitio web otorgó su consentimiento previo y expreso por el solo hecho de que en el sitio se encuentren los términos y condiciones de uso, política de datos, etc., pues ello corresponderá analizarlo a la Dirección de Investigaciones de Protección de Datos Personales de esta entidad dentro de una investigación administrativa" (Superintendencia de Industria y Comercio de Colombia, 2016b).

42 Al respecto, ver los pronunciamientos del magistrado Ciro Angarita Barón sobre la protección efectiva de los derechos que manda la Constitución.

consecuencia, y en respuesta a esa realidad, en la Unión Europea el concepto de "consentimiento" inicialmente incluido en la Directiva 95/46/CE y en la Directiva E-privacy ha tenido que evolucionar. De esta manera, si bien la definición de consentimiento permaneció muy similar en el GDPR,[43] en sus considerandos 32, 42 y 43, y en su artículo 7 se incluyeron lineamientos adicionales para hacerlo exigible.[44]

Así, por un lado, en el numeral 4 del artículo 7 del GDPR se aclaró que

> … al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, *se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato*. (Énfasis agregado)

De esa manera, se excluyó la validez de casos como el citado por el Grupo de Trabajo del Artículo 29 en el Ejemplo No. 1 del documento de trabajo, "Directrices sobre el consentimiento en virtud del Reglamento 2016/679". En dicho ejemplo se describe el caso de una aplicación móvil para edición de fotos que: i) solicita a sus usuarios tener activada su localización de GPS para el uso de sus servicios; ii) le informa a sus usuarios que usará los datos recopilados con fines publicitarios. Dado que ni la

---

Ver por ejemplo, Corte Constitucional, Sentencia T-406 de 1992, M. P. Ciro Angarita Barón.

43 Así, mientras el literal h) del artículo 2 de la Directiva 95/46/CE definía el consentimiento como "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan", el numeral 11 del artículo 4 del GDPR definió el consentimiento como "toda manifestación de voluntad libre, específica, informada *e inequívoca* por la que el interesado acepta, *ya sea mediante una declaración o una clara acción afirmativa*, el tratamiento de datos personales que le conciernen" (énfasis agregado).

44 Cabe aclarar que estos nuevos lineamientos no han sido óbice para que se continúe abusando de la figura del consentimiento. Así, el mismo día de la entrada en vigencia del GDPR (25 de mayo de 2018), la organización Noyb presentó cuatro quejas contra Google (Android), Facebook, WhatsApp e Instagram por "consentimiento forzado", pues en sus "casillas de consentimiento" estaban amenazando al usuario con que el servicio ya no se podría utilizar si los usuarios no daban su consentimiento. Asimismo, el 26 de junio de 2018, el Consejo de Consumidores de Noruega publicó un reporte sobre la manipulación de consentimiento a través del diseño de las interfaces (Noyb, 2018; Forbrukerradet, 2018).

geolocalización ni la publicidad comportamental en línea son necesarios para la provisión del servicio de edición de fotografías, el Grupo de Trabajo considera que dicho caso viola lo establecido en el numeral 4 del artículo 7 antes citado, pues "dado que los usuarios no pueden usar la aplicación sin dar su consentimiento para estos fines, no se puede considerar que el consentimiento sea otorgado libremente".[45]

Por su parte, en el considerando 43 del GDPR se estableció que

> … se presume que el consentimiento no se ha dado libremente cuando *no permita autorizar por separado las distintas operaciones de tratamiento de datos personales* pese a ser adecuado en el caso concreto, o *cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento*, aun cuando este no sea necesario para dicho cumplimiento. (Énfasis agregado)

Y en forma similar, el considerando 32, en su parte pertinente, agregó: "el consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos". De esa manera, el GDPR deja claro que tanto la presentación en bloque de los términos como la condicionalidad de un servicio son indicios de que el consentimiento no ha sido otorgado de manera libre. En esa medida se exige tanto la "granularidad" como la incondicionalidad de los términos y las condiciones, y las políticas de privacidad que se presenten para solicitar el consentimiento del usuario.

Adicionalmente, el considerando 42 del GDPR establece en su parte pertinente que "de acuerdo con la Directiva 93/13/CEE del Consejo (1), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento *con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas*" (énfasis agregado). Como complemento, el Grupo de Trabajo del Artículo 29 ha dicho que "si el consentimiento debe darse por medios electrónicos, la solicitud *debe ser clara y concisa. La información en capas y granular* puede ser una forma adecuada de lidiar con la doble obligación de ser preciso y completo por un lado y comprensible

---

45 Grupo de Trabajo del Artículo 29. *Documento de trabajo "Directrices sobre el consentimiento en virtud del Reglamento 2016/679"*. Adoptado en abril 10 de 2018, 17/EN WP259 rev.01, 6.

por el otro". Así, se sugieren herramientas prácticas para cumplir con la obligación, aún inexistente en Colombia, de presentar la información sobre los tratamientos y las finalidades de manera clara, precisa, concisa y comprensible, según el público al que vaya dirigida.

Por último, es importante notar que a diferencia del literal h) del artículo 2 de la Directiva 95/46/CE ya derogada, el numeral 11 del artículo 4 del GDPR habla de una manifestación de voluntad "*inequívoca* por la que el interesado acepta, *ya sea mediante una declaración o una clara acción afirmativa*, el tratamiento de datos personales que le conciernen" (énfasis agregado). Tal y como lo ha dicho el Grupo de Trabajo del Artículo 29, la consecuencia directa de esta disposición es que "el uso de casillas *opt-in* premarcadas no es válido bajo el GDPR. El silencio o la inactividad por parte del interesado, así como la simple permanencia de un usuario en un servicio no pueden considerarse una indicación activa de elección".[46] Igualmente, "El GDPR no permite a los responsables de tratamiento ofrecer […] construcciones de *opt-out* que requieren una intervención del interesado para evitar un acuerdo (por ejemplo, casillas *opt-out*)".[47]

Como se ve, el ejemplo de la Unión Europea da cuenta de que en Colombia, las condiciones que regulan hoy el consentimiento previo, expreso e informado tienen un amplio campo de mejora para poder considerarse como una verdadera salvaguarda del derecho a la protección de datos de las personas.

Ámbito de aplicación territorial de la ley de protección de datos

Además de establecer si los contenidos de la Ley 1581 de 2012 son suficientes para llamar a rendir cuentas a las EMNBD en el marco de la era digital, también resulta indispensable establecer si el ámbito de aplicación territorial de dicha ley los cobija.

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

46 *Ibid*., 16.
47 *Idem*.

Bajo una interpretación literal de dicho artículo se entendería que, a menos de que les sea aplicable la legislación colombiana en virtud de normas y tratados internacionales, la Ley 1581 de 2012 no es aplicable a las EMNBD *que no tengan domicilio en Colombia*. Lo anterior, pues el tratamiento por ellas hecho se realiza en donde están sus instalaciones (y en consecuencia sus servidores) y no en Colombia. De hecho, así lo consideró inicialmente la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, en su calidad de autoridad de datos personales de Colombia, en el Concepto 14-218349–00003-0000 del 24 de noviembre de 2014, en donde se analizaba si la ley de protección de datos personales colombiana le era aplicable a redes sociales como Facebook. En esa ocasión, la SIC consideró que

> … el tratamiento de los datos personales registrados en las redes sociales no encaja dentro del ámbito de competencia de la Ley 1581 de 2012, pues la recolección, el uso, la circulación, 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*. (Énfasis agregado).

Sin embargo, y aparentemente inspirado en el literal c) [48] del numeral 1° del artículo 4 de la Directiva 95/46/CE, en el Concepto 14-218349–4-0 del 3 de marzo de 2016 la Superintendencia de Industria y Comercio modificó su posición sobre esa cuestión, señalando:

> … Sin duda alguna, el precepto jurídico citado extiende el ámbito de aplicación de la ley estatutaria de protección de datos personales a un sinnúmero de escenarios de tratamiento de información personal en Colombia, verbigracia, de manera

48 Según el cual:
"Artículo 4. Derecho nacional aplicable.
1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: [...]
c) El responsable del tratamiento no esté establecido en el territorio de la Comunidad *y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro*, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.
2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".

> ilustrativa, 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*. (Énfasis agregado)

Entonces, a partir de ese momento quedó claro: i) que la Ley 1581 de 2012 es aplicable a responsables o encargados del tratamiento que estén domiciliados en Colombia; y, ii) que su ámbito de aplicación se extiende también a responsables o encargados no establecidos en el territorio colombiano cuando: a) a estos les sea aplicable la legislación colombiana en virtud de normas y tratados internacionales; o, b) el tratamiento de datos personales en cuestión sea efectuado a través de un "medio" situado en territorio colombiano. Si bien la SIC no lo señaló así, se ha entendido que por "medios" la autoridad de protección de datos se refirió a las llamadas *cookies* que, como vimos, se almacenan en el computador del usuario (ubicado en territorio colombiano) cuando este visita un sitio web.

¿Es ese alcance suficiente para hacer rendir cuentas a las EMNBD que recolectan datos en Colombia?

En el caso de las empresas domiciliadas en Colombia, como son la mayoría de las empresas que en nuestro estudio hacen parte de las *start-ups* y "empresas ya establecidas", es claro que sí lo es. Sin embargo, la situación de las grandes empresas de internet, y de la mayoría de las incluidas bajo la categoría "empresas intermedias" es distinta, pues la mayoría de ellas no tienen domicilio en nuestro país. Si partimos de la base de que todas esas empresas recolectan sus datos a través de las llamadas *cookies*, concluiremos que al menos el tratamiento de recolección se encuentra cubierto por la ley colombiana. No obstante, y tal y como se vio en el capítulo 3 de este documento, es claro que el *web tracking* no es la única fuente de datos utilizada por estas empresas. Adicionalmente, ¿qué sucede con cualquier otra operación o conjunto de operaciones que dichas empresas decidan realizar sobre esos datos personales, como pueden ser el almacenamiento, el uso, la circulación o el cruce con otros datos? En caso de que esos otros tratamientos sean realizados con "medios" ubicados en otro territorio, los mismos quedarían por fuera del ámbito de aplicación territorial de la ley colombiana.

Por eso, 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. En esa medida, su ámbito de aplicación territorial se extendió a todo tipo de tratamiento que se realice sobre los datos personales de "interesados que residan en la Unión", esto es, las "persona[s] física[s] identificada[s] o identificable[s]"[49] que son titulares de los datos.[50]

Además, tanto el artículo 2 de la Ley 1581 de 2012, como la interpretación que la Superintendencia hizo de él se quedan cortos en definir qué sucede cuando el responsable o encargado del tratamiento no está domiciliado en territorio colombiano pero sí tiene allí un establecimiento u otro tipo de representación (filial, sucursal, etc.). A pesar de que, como se verá a continuación, la jurisdicción constitucional colombiana ya tuvo que resolver esta cuestión vía jurisprudencial[51] para poder definir la legitimación pasiva en la causa de varios casos, lo cierto es que brindaría más seguridad jurídica contar con una disposición legal como la que incluía el literal a) del numeral 1° del artículo 4 de la Directiva 95/46/CE ya derogada. De acuerdo con dicho literal, los Estados miembros de la Unión Europea debían aplicar la mencionada Directiva a todo tratamiento de datos personales cuando "el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro". Al interpretar dicha disposición en el caso Google Spain, S.L., y Google Inc., *vs*. Agencia Española de Protección de

---

49 Numeral 1, artículo 4 del GDPR.

50 Así, de acuerdo con el numeral 2° del artículo 3 del GDPR, dicha regulación es aplicable al tratamiento de datos personales *de interesados que residan en la Unión*, por parte de un responsable o encargado no establecido en esta. Sin embargo, la aplicabilidad se encuentra condicionada a que 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.

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

Datos y Costeja González arriba citado, el Tribunal de Justicia de la Unión Europea dejó claro que

> … el artículo 4, apartado 1, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, *cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro*.

En esa medida, se estableció que al responsable del tratamiento de datos no domiciliado en la Unión Europea también le era aplicable la regulación de protección de datos europea cuando contaba con un establecimiento ubicado en su territorio, cuyas actividades se relacionaban con el tratamiento de datos personales hecho por su casa matriz. Así, si bien en el caso bajo estudio el administrador de Google Search era Google Inc., era claro que las actividades de promoción de venta de los espacios publicitarios gestionadas por Google Spain en España se relacionaban con el tratamiento de datos personales hecho en Google Search. De esta manera, la Directiva 95/46/CE era aplicable a dicho tratamiento.

De hecho, a raíz de dicha interpretación, el artículo del ámbito territorial del GDPR fue mucho más explícito en la materia. Así, en el numeral 1° de su artículo 3 se estableció que dicha regulación es aplicable 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*" (énfasis agregado).

Capacidades de las autoridades competentes

Capacidades de regulación, vigilancia, control y sanción de las EMNBD

En Colombia existe una autoridad de protección de datos personales, lo que posiciona al país en una mejor situación frente a otros países como Estados Unidos, en donde dicha calidad ha tenido que ser asumida *de facto* por la Comisión Federal de Comercio (FTC, por sus siglas en inglés) a través de la protección del consumidor. En particular, y haciendo uso de la sección 15 U.S.C. Sec. 45(a)(1) del Federal Trade Commission

Act,[52] la FTC ha protegido a los consumidores digitales de ciertas políticas injustas de recopilación de datos. Por ejemplo, en marzo de 2016 envió cartas de advertencia a los desarrolladores de aplicaciones que permitieron a terceros instalar en sus aplicaciones una pieza de *software* (*audio beacons*) que puede utilizar el micrófono de un dispositivo para escuchar las señales de audio que están incrustadas en los anuncios de televisión, y de esa manera monitorear, con fines de publicidad dirigida, el uso de la televisión por parte de los consumidores (Federal Trade Commission, 2016). Adicionalmente, la FTC ofrece sugerencias en cuanto al grado en que las empresas deben proteger los datos de sus usuarios. Así, trabaja en estrecha colaboración con grupos como Network Advertising Initiative (NAI) y Digital Advertising Alliance (DAA) para "alentar a la industria a proporcionar a los consumidores protecciones básicas de privacidad, incluida la transparencia y el control del consumidor, la seguridad razonable, la retención limitada de los datos del consumidor y el consentimiento expreso afirmativo para el uso de datos sensibles" (Federal Trade Commission, 2017, p. 1). Sin embargo, los principios que la FTC establece no son legalmente vinculantes, y la membresía en la NAI y en la DAA son completamente voluntarias, por lo que las empresas no están obligadas a cumplir con estas sugerencias.

En contraste, en su calidad de autoridad de protección de datos, en Colombia la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, (y la Dirección de Investigación de Protección de Datos Personales que hace parte de ella) ejercen funciones de varios tipos. Por un lado, tiene *funciones regulatorias*, principalmente encaminadas a: i) "promover y divulgar los derechos de las personas en relación con el tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos";[53] ii) "impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los responsables del tratamiento y encargados del tratamiento a las disposiciones previstas"[54] en la ley; iii) "proferir las declaraciones de conformidad sobre las transferencias

52 Según la cual "los actos o prácticas desleales o engañosos en o que afectan al comercio [...] son [...] declarados ilegales".

53 Literal e) del artículo 21 de la Ley 1581 de 2012.

54 *Idem*. Ver también artículos 11 y 27 del Decreto 1377 de 2013.

internacionales de datos";[55] y, iv) "sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional".[56]

Adicionalmente, cuenta con *funciones de control y vigilancia*, tales como: i) "velar por el cumplimiento de la legislación en materia de protección de datos personales";[57] ii) "disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva":[58] iii) "solicitar a los responsables del tratamiento y encargados del tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones",[59] y, en particular, para que demuestren, en virtud del principio de responsabilidad, "que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012"[60] y en su Decreto reglamentario; y, iv) "administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento".[61]

Finalmente, cumple *funciones sancionatorias*, dentro de las que se incluyen: i) "adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos";[62] y, ii) "requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes".[63]

---

55 Literal g) del artículo 21 de la Ley 1581 de 2012. Ver también numeral 5 del artículo 16 del Decreto 4886 de 2011.

56 Literal i), *ibid*.

57 Literal a), *ibid*.

58 Literal c), *ibid*. Ver también numeral 4 del artículo 16 del Decreto 4886 de 2011.

59 Literal f), *ibid*.

60 Artículo 26 del Decreto 1377 de 2013.

61 Literal h) del artículo 21 de la Ley 1581 de 2012.

62 Literal b), *ibid*.

63 Literal j), *ibid*. Ver también numeral 6 del artículo 16 del Decreto 4886 de 2011.

Sin embargo, frente al ejercicio de estas funciones la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio debería tener al menos dos fortalezas. En primer lugar, el talento humano que conforma la Delegatura debería contar con experticia en dos áreas. Por un lado, para poder recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional, y para poder velar por que los operadores y las fuentes tengan sistemas de seguridad y condiciones técnicas suficientes, es necesario contar con funcionarios que tengan competencias para entender el funcionamiento de la explotación de datos, como pueden ser la ingeniería de sistemas, las matemáticas, la estadística, el *machine learning* y el *data science*. Del mismo modo, para poder asegurar que en cada caso concreto se garantice el derecho a la protección de datos personales como un derecho humano, y que se resuelvan las tensiones que este pueda tener con otros, como el derecho al acceso a información pública o la libertad de expresión, es indispensable tener un equipo que cuente con un enfoque de derechos humanos, y no exclusivamente comercial.

En segundo lugar, la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio debe propender por el máximo de autonomía e independencia frente a las empresas a las que debe regular, controlar, vigilar y sancionar, incluidas las EMNBD. Así, y tal como se dijo en la sección de aclaraciones previas, si bien coincidimos con la utilidad y el carácter complementario de las medidas de autorregulación, confiamos también en las virtudes de una regulación puramente estatal o incluso internacional, como la desarrollada en el GDPR. Por eso, en el caso de la Delegatura enfatizamos en que una relación estrecha con los regulados, sin la debida supervisión, es problemática, pues plantea riesgos para la independencia e imparcialidad que el ente regulador debe tener a la hora de ejercer sus funciones de vigilancia, control y sanción.

Competencia frente a las EMNBD

Del apartado referente al ámbito de aplicación territorial de la ley de protección de datos parece claro que, en el caso de Colombia, el ámbito de aplicación de la Ley 1581 de 2012 se extiende a responsables o encargados no establecidos en el territorio colombiano solo cuando: i) les sea aplicable la legislación colombiana en virtud de normas y tratados internacionales; o, ii) el tratamiento de datos personales en cuestión sea efectuado a través de un "medio" situado en territorio colombiano. Pero, ¿cómo se hace efectivo en la práctica ese alcance, si el responsable o el

encargado del tratamiento no están domiciliados en Colombia, como es el caso de Google LLC, Deezer SA o Alibaba Group? ¿A quién llaman las autoridades competentes –sea la Superintendencia de Industria y Comercio o los jueces de la República– a rendir cuentas ante ellos? En últimas, se trata de un tema de legitimación pasiva de quien es llamado a rendir cuentas en materia de tratamiento de datos personales ante la autoridad de protección de datos y ante los jueces colombianos.

En el caso de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, sus actuaciones frente a las EMNBD aquí estudiadas no nos dan muchas luces frente al problema jurídico en cuestión. Lo anterior, pues las únicas empresas de la muestra que han estado sujetas a sanción por parte de la autoridad de protección de datos son las "empresas establecidas" que, como se dijo, suelen tener domicilio en Colombia. Así, al revisar la base de datos de sanciones de la Delegatura para la Protección de Datos Personales,[64] que incluye las sanciones impuestas entre 2014 y 2018 por tratamientos inadecuados de datos personales, se constató que Almacenes Éxito S.A. (2), Telmex Colombia S.A. (1) y Grupo Aval Acciones y Valores S.A. (a través del Banco de Occidente S.A) (1) son las únicas empresas de la muestra con sanciones impuestas.

Por un lado, Almacenes Éxito S.A. fue inicialmente sancionado el 30 de mayo de 2014 (Superintendencia de Industria y Comercio, 2014a) por no corregir el nombre de una de sus clientes, el cual se encontraba mal incorporado en la base de datos del programa de fidelización "Superclientes Carulla", y no informarle en dónde podía encontrar la política de tratamiento de datos personales. Asimismo, el 25 de junio de 2018 (Superintendencia de Industria y Comercio, 2018a) esta sociedad fue nuevamente sancionada, esta vez por omitir suprimir la dirección de correo electrónico de una de sus clientes y continuar enviándole correos electrónicos con contenido publicitario, aun en contra de la voluntad de la titular. Por su parte, el Banco de Occidente S.A, sociedad que hace parte del Grupo Aval Acciones y Valores S.A., fue sancionado el 13 de diciembre de 2016 (Superintendencia de Industria y Comercio, 2016c) por no contar con el soporte correspondiente de los consentimientos dados por sus clientes para: i) utilizar su correo electrónico para enviarles un correo

64 Superintendencia de Industria y Comercio (2018b). Sanciones de protección de datos personales. Disponible en http://www.sic.gov.co/sanciones-2018

promocional de un esquema de financiación de créditos; ni ii) divulgar masivamente dichos correos electrónicos con otros titulares. Por último, la empresa Telmex Colombia S.A. fue sancionada el 30 de noviembre de 2017 (Superintendencia de Industria y Comercio, 2017) por no suprimir de sus bases de datos el correo electrónico de una persona que no era cliente de esta sociedad, lo que permitió que siguiera recibiendo mensajes de facturación de una cuenta de la que no era titular.

Así, si bien estos casos son útiles para hacerse una idea del tipo de problemáticas que aborda la Superintendencia en el marco de la era digital (principalmente relacionadas con correos electrónicos y con publicidad dirigida por medios digitales), los mismos no permiten establecer la posición de la autoridad de protección de datos frente a la legitimación pasiva del responsable de tratamiento que, sin tener domicilio en Colombia, es llamado a rendir cuentas en nuestro país.

Sin embargo, el ejercicio –aunque escaso– por parte de la SIC de la función consagrada en el literal j) del artículo 21 de la Ley 1581 de 2012, parece mostrar la intención de nuestra autoridad de protección de datos personales de hacer rendir cuentas a las EMNBD sin domicilio en Colombia por medio de la cooperación internacional. De acuerdo con el mencionado literal, entre las funciones de la SIC se encuentra la de "requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales". Del mismo modo, el numeral 6 del artículo 16 del Decreto 4886 de 2011 incluye dentro de las funciones del Despacho del superintendente delegado para la protección de datos personales la de "requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales". Haciendo uso de dicha función, en época del superintendente delegado José Alejandro Bermúdez se adelantaron inspecciones de compañías en Colombia cuyo tratamiento de datos personales tenía la potencialidad de afectar a ciudadanos en España.[65] Así, si bien aún no contamos con evidencia de casos

65 Esta información fue obtenida gracias a la participación del exsuperintendente delegado José Alejandro Bermúdez en el grupo focal realizado el 20 de noviembre de 2018 con motivo de la publicación de este documento. Para consultar la lista de los demás asistentes, ver Anexo 3 del presente documento.

de cooperación para inspeccionar EMNBD extranjeras con potencialidad de afectar a ciudadanos colombianos, esta parece ser la opción hasta ahora explorada por la SIC.

En lo que respecta a la Corte Constitucional, en su calidad de juez encargado de la protección efectiva del derecho a la protección de datos personales, su posición frente a la legitimación pasiva de las EMNBD sin domicilio en Colombia ha sido más explícita. En concreto, y tal como se verá a continuación, la Corte se ha tenido que enfrentar al problema de la legitimación pasiva de Google Inc (hoy Google LLC)[66] en tres ocasiones. Infortunadamente, en ninguno de esos casos la Corte ha analizado la violación del derecho a la protección de datos personales, ya sea porque se trataba de información periodística (a la que no le es aplicable la Ley 1581 de 2012, aunque sí sus principios rectores) o porque ha determinado, de forma inexplicable y finalmente fallida, que lo que está en juego son los derechos del consumidor. A pesar de esta oportunidad perdida, el contenido de estas tres sentencias continúa siendo útil para efectos de analizar cómo se ha llamado a rendir cuentas en Colombia a las empresas de ese tipo que carecen de domicilio en el país.

El primer caso, ya citado en este documento, se dio en el año 2013. En ese caso, un hombre instauró una acción de tutela contra Google Colombia Ltda. y contra la Casa Editorial El Tiempo S.A, solicitando que con el fin de proteger sus derechos fundamentales se le ordenara a las entidades demandadas eliminar de los registros del periódico y de Google Search el artículo titulado "Los hombres de la mafia en los Llanos", en el que él aparecía mencionado. En esa ocasión, Google Colombia Ltda. respondió la demanda aduciendo los siguientes argumentos: i) "Google Colombia tiene como objeto comercial 'la venta, distribución, comercialización y desarrollo, en forma directa o indirecta, de productos y servicios de *hardware* y *software*, productos y servicios relacionados a internet y publicidad en internet o por cualquier otro medio', en ese sentido, Google Colombia no es la entidad responsable de las acusaciones que se presentan por el actor, en razón de que no es quien administra el servicio del buscador de Google Inc.";[67] ii) "el proveedor de servicios de búsquedas, no es responsable del contenido de las páginas que figuren como resultados

66 En septiembre de 2017 Google pasó de ser una corporación, a ser una compañía de responsabilidad limitada (LLC, por sus siglas en inglés).

67 Corte Constitucional, Sentencia T-040 de 2013, M. P. Jorge Ignacio Pretelt Chaljub.

de búsquedas, ni tampoco es responsable como erróneamente lo afirma el accionante por 'mantener en sus registros' determinada información".[68] Así, por primera vez se elevó el argumento de la diferencia de objeto social existente entre Google Colombia Ltda. y Google Inc., este último como el proveedor de servicios de búsqueda y, en esa medida, el presunto encargado de tratamiento de los datos que allí aparecen.

Infortunadamente, y tal y como se expuso *in extenso*, al revisar la legitimidad por pasiva de la acción de tutela, la Corte Constitucional solo se refirió al segundo argumento aducido por la compañía concerniente a que el responsable de la información emitida, y por ende de su posible rectificación, es el medio de comunicación que recolectó, analizó, procesó y divulgó la noticia, es decir, la casa Editorial El Tiempo, a través de su página electrónica oficial. En esa medida, consideró que

> … Google Colombia S.A. no es responsable de la noticia "Los hombres de la mafia de los Llanos", pues como bien lo explicó esta empresa en el escrito de contestación, Google presta un servicio de búsqueda de la información que hay en toda la red, y no es quien redacta o publica tal información, sino que es un simple motor de búsqueda al cual no se le puede endilgar la responsabilidad sobre la veracidad o imparcialidad de un respectivo artículo, noticia o columna que aparezca en sus resultados.[69]

De esa manera, evadió el abordaje del problema jurídico de la personería jurídica de Google Inc. en Colombia, refiriéndose de manera general a "Google".

Tiempo después el problema jurídico en cuestión volvería a surgir. Ese caso –también descrito en páginas anteriores–, se trató de una mujer llamada por la Corte "Gloria", que interpuso una acción de tutela contra la Casa Editorial El Tiempo solicitando que se le ordenara a la accionada bajar y borrar de todos los motores de búsqueda disponibles y, específicamente, de Google.com una nota periodística en la que se informaba sobre la supuesta participación de la accionante en hechos constitutivos de delito de trata de personas. A pesar de que dentro de los demandados no se incluyó a Google Colombia Ltda., la Sala Primera de Revisión de la Corte Constitucional ordenó vincular a esta compañía al proceso, para que se pronunciara sobre los hechos y las pretensiones de la acción constitucional. En

---

68 *Idem*.

69 *Idem*.

forma similar al caso anterior, al responder la demanda Google Colombia Ltda. señaló que "carece de legitimación por pasiva, al no ser esta compañía una sucursal ni representar jurídicamente a Google Inc., por lo que de impartirse una orden a Google Inc., esta no podría ser cumplida por Google Colombia, al no tener control sobre las acciones de su sociedad matriz".[70] Lo anterior, en la medida en que "el manejo y control del buscador de Google y de los dominios www.google.com y www.google.com.co corresponde a Google Inc., compañía constituida en los Estados Unidos de América y con domicilio en dicho país". Asimismo, reiteró que la única responsable de la publicación es la Casa Editorial El Tiempo, titular del portal de internet donde se encuentra dicho contenido, y quien puede decidir qué parte de este puede ser indexado por los motores de búsqueda.

Sin embargo, una vez más la Corte Constitucional evitó referirse a la personería jurídica de Google Inc. en Colombia, aduciendo en cambio que "ordenar al motor de búsqueda Google.com que bloquee de sus resultados el portal de Internet del medio de comunicación donde se informa de la captura e investigación penal en contra de Gloria, supondría implementar una modalidad de control previo contraria al principio de neutralidad".[71] De esa manera la Corte pasó por alto que, en todo caso, en el asunto bajo estudio resultaba procedimentalmente imposible ordenarle a quien maneja y controla ese buscador el bloqueo de determinados resultados, pues dicha persona jurídica no había sido vinculada al proceso.

Un tercer caso se conocería en febrero de 2017. En esa ocasión, un hombre interpuso una acción de tutela contra Google Inc. y Google Colombia Ltda. para obtener la protección de sus derechos fundamentales a la intimidad, al buen nombre y a la honra, los cuales consideraba vulnerados como consecuencia de una publicación anónima en un blog de internet de la plataforma www.blogger.com –de propiedad de la compañía Google Inc.–, en la que se afirmaba que la empresa Muebles Caquetá, de propiedad del accionante, y su propietario, estafaban a sus clientes. Al ser la primera vez que se demandaba a Google Inc., la contestación de este accionado fue presentada por la firma de abogados Gómez-Pinzón Zuleta Abogados, en calidad de agente oficioso de Google Inc. Al respecto, la firma de abogados señaló que

---

70 Corte Constitucional, Sentencia T-277 de 2015, M. P. María Victoria Calle Correa.

71 *Idem*.

> … la calidad de agente oficioso, en los términos del artículo 57 del CPC (sic), se hace necesaria en la medida en que (i) está en proceso el otorgamiento en el extranjero de poder correspondiente y necesario, y (ii) en consideración al domicilio, en Mountain View, California, Estados Unidos, le es imposible a Google Inc. contestar la demanda de la referencia.[72]

Posteriormente, y una vez otorgado el correspondiente poder por la compañía demandada a la referida firma de abogados, esta última manifestó obrar como apoderado judicial de Google Inc. en Colombia con poder especial, amplio y suficiente para representarla "en el proceso de la referencia".

Sin poner reparos sobre la agencia oficiosa ni sobre la posterior representación legal de Google Inc. por parte de la firma de abogados Gómez-Pinzón Zuleta Abogados, la Corte ordenó a Google Inc., en su calidad de propietaria de "Blogger.com" que dentro del mes siguiente a la notificación de la sentencia, eliminara el blog con dirección http://muebles-caqueta.blogspot.com.co, por cuanto su contenido imputaba de forma anónima información no probada sobre la comisión del delito de estafa y otras expresiones que podían considerarse calumnias contra el demandante y su empresa, y dado que este último no contaba con otro recurso efectivo para obtener su pretensión. Asimismo, le advirtió que, mientras no regulase la materia de los blogs anónimos con contenido difamatorio, desproporcionado, calumnioso o injurioso en la política de contenidos de su herramienta "Blogger.com", en los casos en donde el afectado por esta clase de blogs demostrara no tener la posibilidad de defenderse, controvertir o rectificar en igualdad de condiciones la información allí contenida por la naturaleza anónima de la publicación, debería proceder a eliminar el contenido denunciado sin exigir una orden judicial previa.

Por último, y a pesar de que en su contestación la empresa Google Colombia Ltda. volvió a reiterar su falta de legitimación pasiva pues "'Google Colombia Ltda.' y 'Google Inc.' son dos entidades independientes, cada una con domicilio, personería jurídica y objetos sociales diferentes", en esta ocasión la Corte Constitucional señaló lo siguiente, que por su importancia para el objeto del presente documento se transcribe *in extenso*:

---

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

La primera consideración tiene que ver con una precisión que resulta necesario hacer entre las dos entidades demandadas en el presente caso: Google Inc. y Google Colombia Ltda. En efecto, la orden antes reseñada se va a dirigir principalmente contra la compañía Google Inc. en la medida en que aunque también fue demandada Google Colombia Ltda., esta última señaló en el trámite de revisión que no representa los intereses legales ni corporativos de Google en Colombia, sino solamente "es una agencia de gestión y venta de publicidad de Google, que tiene tanto personería jurídica como objeto social independiente". Sin embargo, a este respecto, deben realizarse varias observaciones:
(i) Si bien la Corte entiende que se trata del ejercicio de funciones comerciales y administrativas diferentes bajo el amparo de la misma marca, esto no es óbice para que Google Colombia Ltda. no pueda acompañar la gestión del cumplimiento de las órdenes que se den a Google Inc., máxime cuando *esta última es su compañía matriz y cuenta con participación accionaria en su filial colombiana,* tal y como lo acredita a folio 45 del expediente el certificado de existencia y representación legal de Google Colombia Ltda.
(ii) En este mismo sentido resulta necesario advertir que *ambas compañías (tanto Google Inc. como Google Colombia Ltda.) al ejercer actividades en Colombia están obligadas a respetar los derechos de los usuarios y consumidores de servicios de telecomunicaciones e internet en el país*, tal y como lo señala la Constitución, la legislación vigente (Ley 1341 de 2009 y Resolución 5111 de 2017 de la Comisión Nacional de Comunicaciones) y los capítulos 14 (Telecomunicaciones) y 15 (Comercio Electrónico) del Tratado de Libre Comercio suscrito entre Colombia y EE.UU. en materia de protección de los derechos de los usuarios y consumidores de servicios de telecomunicaciones e Internet.
(iii) De forma complementaria, resulta necesario resaltar que *la presencia territorial de Google en Colombia no comporta únicamente una representación comercial aislada, también implica responsabilidades legales y administrativas con las autoridades colombianas cuando se trata de garantizar los derechos de los usuarios de los servicios de telecomunicaciones e Internet que han sido amparados por sentencias de tribunales nacionales competentes.* A este respecto, vale la pena recordar que en varios países como Inglaterra (Tamiz *vs*. Google Inc. - 2014), Australia (Trkulja *vs*. Google Inc. - 2015), Canadá (Pia Grillo c. Google Inc. - 2014), Brasil (Daniela Cicarelli *vs*. Google Inc. - 2015) y la región admi-

> nistrativa especial de Hong Kong (Yeung *vs.* Google Inc. - 2014 y Oriental Press Group *vs.* Fevaworks Solutions - 2013), entre otros, la compañía Google Inc. y sus subsidiarias locales han enfrentado similares controversias en las que se les ha ordenado en conjunto cumplir con diversos mandatos judiciales por casos de difamación en páginas web, buscadores y blogs que atentan contra los derechos de los usuarios y consumidores de servicios de telecomunicaciones e internet.[73] (Énfasis agregado)

Con base en esas premisas, la Corte le ordenó: i) a Google Colombia Ltda., realizar todas las actividades que fueran necesarias para lograr que Google Inc. retirase el contenido objeto del litigio y enviar informe de tal retiro a la Corte Constitucional dentro del mes siguiente a la notificación de la presente providencia; ii) a ambas empresas, que "en su calidad de *proveedores de servicios de telecomunicaciones e Internet en Colombia,* se inscriban en el registro TIC a cargo del Ministerio de Tecnologías de la Información y las Comunicaciones, tal y como lo establece la Ley 1341 de 2009 (art. 15) para compañías cuyas actividades y objeto corresponden al sector TIC con el objeto de ofrecer mayores garantías para la protección de los derechos de los usuarios y consumidores de servicios de telecomunicaciones e Internet en el país".[74]

A partir de dicho fallo, y tal y como quedaría evidenciado en la Sentencia T-121 de 2018 fallada un tiempo después, parecía que se había zanjado la discusión sobre la legitimación por pasiva de Google Inc. en los casos de presunta violación de derechos en el ámbito de los productos que ofrece en Colombia la referida compañía (el motor de búsqueda, o la plataforma YouTube, como es el caso de la Sentencia T-121 de 2018). De esta manera, parecía claro que cuando empresas de este tipo sin domicilio en Colombia fueran llamadas a rendir cuentas ante las autoridades competentes colombianas: i) serían *al menos* responsables frente a la protección de los derechos de los usuarios y consumidores de servicios de telecomunicaciones e internet en el país (pues como de vio más arriba, la responsabilidad frente al tratamiento de datos personales de este tipo de empresas sigue aún sin ser abordada); ii) debían nombrar a un apoderado para que las representara en el país; y, iii) sus establecimientos en Colombia serían también responsables.

---

73 *Idem*.

74 *Idem*.

Sin embargo, mediante el Auto 285 de fecha 9 de mayo de 2018, la Corte falló a favor de la solicitud de nulidad presentada por Google Colombia Ltda., Google LLC (antes Google Inc.)[75] y el MinTIC contra la sentencia antes citada. Así, se declaró la nulidad de la mencionada providencia por violación del debido proceso, por considerar que en la misma se omitió el análisis de tres asuntos de relevancia constitucional cuya revisión hubiese podido influir en la determinación adoptada y las órdenes impartidas de manera que la decisión hubiere sido distinta. Por un lado, la Corte consideró que la sentencia no abordó la prohibición de la censura consagrada en el artículo 20 superior, lo que lleva a que el ordinal segundo de la parte resolutiva del fallo habilite una especie de censura sin orden judicial previa, al imponer sobre Google una obligación de monitoreo constante para la eliminación automática de contenido que se realice sobre una misma temática.

En segundo lugar, se estableció que se dejó de lado el estudio sobre la diferencia entre la persona que crea el contenido y lo publica, y el propietario de la herramienta que solo facilita la publicación, lo que propició que las determinaciones adoptadas en torno de la publicación fueran exclusivamente dirigidas a Google LLC, sin presentar una motivación adecuada que así lo respaldase. Según la Corte, "la responsabilidad del creador del contenido de las afirmaciones calificadas como difamatorias, desproporcionadas y calumniosas en la referida providencia, no es equiparable al rigor en el trato proporcionado a los intermediarios en internet que sirvieron como medio para alojar el contenido vejatorio".[76]

Finalmente, se consideró que la sentencia en comento había dejado de abordar que Google LLC hace parte de la categoría proveedores de contenidos y aplicaciones (PCA) y no de la categoría de proveedores de redes y servicios de telecomunicaciones (PRST). Según la Corte, el haber agotado este aspecto hubiera permitido llegar a una decisión diferente, en particular en lo que respecta a las disposiciones resolutorias relacionadas con la inscripción en el registro TIC y el monitoreo del MinTIC a las actividades adelantadas por Google LLC.

---

75 Como se dijo, en septiembre de 2017 Google pasó de ser una corporación, a ser una compañía de responsabilidad limitada (LLC, por sus siglas en inglés).

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

Así, si bien entre las causales de nulidad aducidas por la Corte no se incluyó el tema de la representación legal de Google LLC en Colombia, ni de la responsabilidad compartida que se le exigió asumir a su filial colombiana, lo cierto es que la totalidad de la Sentencia T-063A de 2017 fue finalmente anulada. En esa medida, actualmente no existe un precedente judicial en Colombia que precise la forma en la que se puede llamar a rendir cuentas a las EMNBD que carecen de domicilio en el país.

CONCLUSIONES Y RECOMENDACIONES

Después de este recorrido por la forma de operar de nuestra muestra de EMNBD, por los vacíos y las falencias del régimen de protección de datos personales colombiano, y por las capacidades de las autoridades competentes para hacer rendir cuentas a las EMNBD, podemos llegar a las siguientes conclusiones.

Por un lado, la forma de operar de las empresas aquí estudiadas da cuenta de los retos que la era digital, la economía digital y el *big data* plantean para los derechos a la protección de datos, a la intimidad y a la igualdad, y para las libertades relacionadas. Así, los grandes volúmenes de datos digitales, junto con las técnicas de analítica de datos hoy existentes le han permitido a las empresas contar con nuevas fuentes de información (en las que sobresalen las *cookies* como herramienta tecnológica para hacer *web tracking*), con nuevos tratamientos de datos (sin que haya suficiente transparencia sobre el funcionamiento de los algoritmos y demás herramientas tecnológicas utilizadas para hacer análisis descriptivo, predictivo y prescriptivo de datos) y, sobre todo, con nuevas finalidades (siendo la comercialización de datos, la provisión de contenidos personalizados y la toma de decisiones automatizas las finalidades más innovadoras, todas ellas con la práctica del *profiling*, ya sea como herramienta o como objetivo).

Por su parte, dichas nuevas fuentes, tratamientos y finalidades, y, en particular, el uso recurrente de *cookies*, algoritmos y del *profiling*, dan cuenta también de las deficiencias que tiene nuestro régimen de protección de datos actual para lidiar con los cuatro riesgos mencionados en la introducción de este documento, y que según el Grupo de Trabajo del Artículo 29 plantean preocupaciones en el marco de la era digital. Al respecto, es importante notar que las mencionadas deficiencias tienen que ver tanto con la existencia de regulación inadecuada, como con la inexistencia de

regulación alguna, o, en el mejor de los casos, con la presencia de disposiciones que, si bien tienen el potencial de abarcar temas y conceptos propios de la era digital, deben ser adecuadamente interpretadas para el efecto.

Además, se constata la existencia de una ley de protección de datos personales cuyo ámbito de aplicación territorial es insuficiente en el marco de la era digital. Lo anterior, pues la interpretación de su alcance actual se queda corta frente a los tratamientos de datos personales hechos con "medios" ubicados fuera del país. Asimismo, dicho alcance no es claro frente a responsables de tratamiento que, si bien no tienen domicilio en el país, sí tienen un establecimiento ubicado en Colombia.

Por último, se encuentran unas autoridades competentes con niveles de alistamiento disímiles. Por un lado, una autoridad de protección de datos con capacidades técnicas insuficientes para tratar temas de explotación de datos y de balance entre derechos humanos, con límites difusos frente al tipo de relación que es necesario mantener con los sujetos a los que debe regular, controlar, vigilar y sancionar, con un enfoque en el control, la vigilancia y la sanción de las EMNBD "establecidas", más que en las que han surgido como respuesta a la era digital,[1] y con apenas tímidos ejercicios de la función de cooperación internacional que la ley le ordena ejercer cuando se afecten los derechos de los titulares de los datos personales fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales. Por su parte, una Corte Constitucional que si bien se siente empoderada y parece tener la intención de hacer rendir cuentas a las EMNBD, aún no encuentra los argumentos jurídicos

1 Al respecto, cabe decir que esta característica resulta contradictoria frente la posición expresada por la Superintendencia de Industria y Comercio en la *Guía para la implementación del principio de responsabilidad demostrada (Accountability)*. Según esta guía: "Teniendo en cuenta que los recursos de vigilancia de la autoridad de protección de datos personales son limitados, *su práctica supervisora debe enfocarse hacia aquellas entidades subestándar, con mayores niveles de riesgo, donde el tratamiento de la información genera un riesgo sistemático con la potencialidad de afectar de manera grave a los titulares*" (énfasis agregado) (Superintendencia de Industria y Comercio, s. f., p. 7). Sin decir en ningún momento que las EMNBD incluidas en las categorías de *Startups* y de "empresas intermedias" son subestándar, lo cierto es que las relaciones de intercambio de datos que, como vimos, estas empresas suelen mantener con los Gafam, hacen que el tratamiento de datos personales por ellas realizado pueda plantear mayores riesgos para el derecho a la protección de datos personales que los planteados por las "empresas establecidas".

correctos,[2] y sigue sin recurrir al derecho a la protección de datos personales para hacerlo.

Entonces, siendo conscientes del campo de mejora que existe para garantizar los derechos y las libertades de los colombianos en la era digital, y buscando poner a Colombia a tono con la normativa de protección de datos más garantista hasta el momento, en el presente documento consideramos necesario:

1. Que se ahonde, por hacer falta en este texto elementos de análisis suficientes, en la investigación académica sobre el alcance y las posibles repercusiones que pueden tener sobre los derechos y libertades de los colombianos:
   a. El poder y el control que los Gafam tienen sobre la mayoría de las aplicaciones y plataformas más populares en Colombia, y el intercambio interno e irrestricto de datos que se permite entre los productos del mismo grupo empresarial.
   b. Las relaciones que existen entre los Gafam y las demás EMNBD en virtud de los inicios de sesión compartidos y de la inserción de botones sociales de Twitter, Google+, LinkedIn o Facebook en la página o aplicación de las EMNBD.
2. Que se promueva un *mayor desarrollo doctrinal y jurisprudencial* sobre:
   a. El concepto de *dato personal* consagrado en el literal c) del artículo 3 de la Ley 1581 de 2012, para que quede claro si incluye otras acepciones de dato personal como el IP y los identificadores similares o los datos asociados a ellos.
   b. El concepto de *dato sensible* establecido en el artículo 5 de la Ley 1581 de 2012, para que quede claro si 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.
   c. El posible carácter de responsables de tratamiento de datos personales que pueden tener los creadores de contenido, los intermediarios de internet y quienes realizan *web crawling*, y, en su defecto, la rendición de cuentas respecto de dicho trata-

2 Esto, pues tal y como se vio con el Auto 285 de 2018, la protección de los derechos de los usuarios de los proveedores de redes y servicios de telecomunicaciones no parece ser la vía adecuada.

miento que deben realizar dichos creadores, intermediarios y *web crawlers.*

d. La forma en la que se puede llamar a rendir cuentas a EMNBD que carecen de domicilio en el país.

Evidentemente, dicho desarrollo doctrinario y jurisprudencial dependerá de un mayor involucramiento de la ciudadanía y de la sociedad civil por medio del litigio, y de la presentación de quejas y solicitudes de conceptos ante la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio. Si bien somos conscientes de que en virtud del artículo 28 de la Ley 1437 de 2011 los conceptos emitidos por la Delegatura no son de obligatorio cumplimiento o ejecución, lo cierto es que los mismos constituirán una guía tanto para los jueces como para los sujetos obligados de la ley, sobre el alcance de dichos términos e interrogantes.

3. Que se dé *un mayor desarrollo doctrinal, reglamentario, legal o jurisprudencial* sobre las siguientes prácticas:
   a. 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: i) sean esenciales para el funcionamiento del servicio solicitado; o, ii) recolecten datos anonimizados o para uso agregado.
   b. 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.
   c. Los tratamientos de datos que tengan como finalidad la *comercialización de datos*, la *provisión de contenidos personalizados* (en particular cuando se trate de publicidad comportamental) y la *toma de decisiones automatizadas*, 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.
   d. La posibilidad de *compartir datos personales sensibles para fines de investigación*, para que se impongan mayores restricciones a dicho intercambio de datos, que no solo incluyan su anonimización, sino también el cumplimiento de los cuatro criterios del test de compatibilidad propuesto por el Grupo de Trabajo del Artículo 29.

e. 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.

4. Que *se reforme la Ley 1581 de 2012*, en lo que tiene que ver con:
   a. El ámbito de aplicación territorial de la Ley, para que deje de depender de la ubicación que tengan el responsable o encargado del tratamiento, sus establecimientos o los medios que utilice para tratar los datos, y pase a depender de la ubicación de los titulares de los datos personales que son objeto de tratamiento.
5. Que se dote a la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio de mayores capacidades técnicas y de talento humano especializado tanto en explotación de datos como en derechos humanos, para poder hacer frente a los retos tecnológicos y de derechos humanos que plantea la regulación del *big data* y del tratamiento de datos personales en el marco de la era digital.
6. Que se incentive el uso, por parte de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, de la función de cooperación internacional con las autoridades de protección de datos de otros países cuando se afecten los derechos de los titulares fuera del territorio colombiano con ocasión de la recolección internacional de datos personales.
7. Que las EMNBD complementen sus medidas de autorregulación con la incorporación, en sus políticas de privacidad, de las mejores prácticas identificadas en las políticas de privacidad aquí revisadas, como pueden ser:
   a. Que el contenido de los mensajes que el usuario envía por medio de la aplicación o plataforma no se guarde en los servidores de la EMNBD, sino en el dispositivo del usuario (práctica identificada en las políticas de privacidad de las aplicaciones WhatsApp y 30 Days Fitness Challenge).
   b. Que los datos sobre la ubicación del usuario se recolecten de forma anónima (práctica adoptada por Apple).

c. Que, en lo posible, los datos recolectados a través de *web tracking* (*log data* y *online data*) solamente sean utilizados en forma agregada o estadística, es decir, para informarle a los socios y aliados de la EMNBD sobre la manera en que los usuarios, colectivamente considerados, utilizan los servicios (práctica identificada en la política de privacidad de la plataforma Cívico).
d. Que al recibir datos de terceros se exija que estos últimos cuenten con derechos legítimos para recopilar, usar y compartir esa información (práctica adoptada por Facebook y Fluvip).
e. Que al compartir datos con terceros se les exija que respeten las instrucciones de la EMNBD y cumplan con sus condiciones en el momento de usar la información en su nombre (práctica identificada en la política de privacidad de WhatsApp y Aliexpress).
f. Que se especifiquen las clases de *cookies* que utiliza la EMNBD para recolectar información (práctica identificada en las políticas de privacidad de Apple, 1Doc3, Biko, Tinder, Netflix).
g. Que las *cookies* de análisis o de comportamiento, y las de funcionalidad, solo recolecten información de forma anónima (práctica adoptada por Apple).
h. Que en caso de una reorganización, reestructuración, fusión o venta, o cualquier otra transferencia de bienes de la EMNBD, la transferencia de la información, incluida la personal, esté sujeta a que el destinatario se comprometa a respetar la información personal de conformidad con la política de privacidad de quien recolectó los datos (práctica identificada en las políticas de privacidad de AliExpress y Netflix).
i. Que se hagan públicos los nombres de las aplicaciones de terceros que se conectan a la aplicación de la EMNBD o que se utilizan para iniciar sesión en ella, así como de los socios de medición con los que se comparte información (práctica identificada en la política de privacidad de la aplicación 8fit Workouts and Meal Planner).

Si bien estas recomendaciones implican cambios en varios niveles, es indispensable que se empiecen a desarrollar lo más pronto posible. Esto, para asegurar que las EMNBD comiencen a rendir cuentas en Colombia antes de que su creciente poder económico, tecnológico y social las haga imposibles de controlar.

GLOSARIO

A continuación se presenta la definición de algunos términos técnicos que han sido mencionados a lo largo del texto.

Algoritmo: "serie ordenada de instrucciones, pasos o procesos que llevan a la solución de un determinado problema. Estos permiten describir claramente una serie de instrucciones que debe realizar una máquina para lograr un resultado previsible" (TICbeat, 2017).

Cookie: "información almacenada en su computadora sobre documentos de internet que ha visto" (Cambridge Dictionary, s. f.).

Data broker: "persona o empresa cuyo negocio es vender información sobre compañías, mercados, etc." (Cambridge Dictionary, s. f.).

Data mining: "proceso de detectar la información procesable de los conjuntos grandes de datos. Utiliza el análisis matemático para deducir los patrones y tendencias que existen en los datos" (TICbeat, 2017).

Datos biométricos: datos capturados a partir de "las tecnologías que miden y analizan las características del cuerpo humano, como el ADN, las huellas dactilares, la retina y el iris de los ojos, los patrones faciales o de la voz, y las medidas de las manos a efectos de autenticación de la identidad" (TICbeat, 2017).

Des-taggear: "[Des-][m]arcar una información digital para [que no sea] procesada de una manera particular" (Cambridge Dictionary, s. f.).

Dirección de Protocolo de Internet (Dirección IP): "número que identifica, de manera lógica y jerárquica, a una interfaz en red

(elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, *smartphone*) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP" (TICbeat, 2017).

Geolocalización: "tecnología que muestra el lugar donde se encuentra cuando utiliza internet o un teléfono móvil" (Cambridge Dictionary, s. f.).

Interfaz de Programación de Aplicaciones (API, por sus siglas en inglés): "conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro *software* como una capa de abstracción" (TICbeat, 2017).

Localizador uniforme de recursos (URL, por sus siglas en inglés): "dirección de sitio web" (Cambridge Dictionary, s. f.).

Machine learning: "disciplina científica del ámbito de la inteligencia artificial que crea sistemas capaces de aprender de forma automática" (TICbeat, 2017).

Open data: "filosofía y práctica que persigue que determinados tipos de datos estén disponibles de forma libre para todo el mundo, sin restricciones de derechos de autor, de patentes o de otros mecanismos de control" (TICbeat, 2017).

Opt in: "elegir ser parte de una actividad, arreglo, etc." (Cambridge Dictionary, s. f.).

Opt ut: "elegir no ser parte de una actividad o dejar de participar en ella" (Cambridge Dictionary, s. f.).

Profiling o generación de perfiles: "práctica o método de seleccionar un conjunto de características pertenecientes a una determinada clase o grupo de personas o cosas por las cuales identificar individuos como pertenecientes a dicha clase o grupo" (Diccionario Collins, s. f.).

Sistema de posicionamiento global (GPS, por sus siglas en inglés): "sistema que puede mostrar la posición exacta de una persona o cosa mediante el uso de señales de satélites" (Cambridge Dictionary, s. f.).

REFERENCIAS

Alcaíno, M., Arenas, V. y Gutiérrez, F. (2015). *Modelos de negocios basados en datos: desafíos del big data en Latinoamérica*. Chile: Universidad de Chile.

App Annie (2017). *Top App Matrix*. Recuperado de https://www.appannie.com/dashboard/home/

BNamericas (20 de julio 2017). *Ranking de aseguradoras colombianas*. Recuperado de http://www.bnamericas.com/es/noticias/seguros/ranking-de-aseguradoras-colombianas/

Cambridge Dictionary (s. f.) Disponible en https://dictionary.cambridge.org/es/

Colombia Digital (2013). *Infografía: "*¿Cómo están posicionados los gigantes de Internet? Recuperado de https://colombiadigital.net/images/infografias/como-estan-posicionados-los-gigantes-de-internet.jpg

Comisión Europea (1998). Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. *Documento de trabajo DG XV D/5057/97: Evaluación de la autorregulación industrial: ¿en qué casos realiza una contribución significativa al nivel de protección de datos de un país tercero?* Adoptado el 14 de enero de 1998.

Corredor, G. R. (2015). Consolidación de la economía digital y desafíos en materia de protección de la privacidad. *Revista de derecho, comunicaciones y tecnologías,* 14, 1-26.

Corte Constitucional, Sentencia T-222 1992, M. P. Ciro Angarita Barón.

Corte Constitucional, Sentencia T-406 de 1992, M. P. Ciro Angarita Barón.

Corte Constitucional, Sentencia T-414 de 1992, M. P. Ciro Angarita Barón.

Corte Constitucional, Sentencia T-729 de 2002, M. P. Eduardo Montealegre Lynett.

Corte Constitucional, Sentencia C-150 de 2003, M. P. Manuel José Cepeda Espinosa.

Corte Constitucional, Sentencia C-748 de 2011, M. P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional, Sentencia T-040 de 2013, M. P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional, Sentencia T-277 de 2015, M. P. María Victoria Calle Correa.

Corte Constitucional, Sentencia C-542 de 2015, M. P. Humberto Antonio Sierra Porto.

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

Corte Constitucional, Sentencia T-121 de 2018, M. P. Carlos Bernal Pulido.

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

Datta, A., Tschantz, M.C. y Datta, A. (2015). Automated Experiments on Ad Privacy Settings. *Proceedings on Privacy Enhancing Technologies,* 1, pp. 92-112.

De Mauro, A., Greco, M. y Grimaldi, M. (2014). *What is Big Data? A Consensual Definition and a Review of Key Research Topics.* Documento presentado en la 4ta Conferencia Internacional sobre Información Integrada, Madrid, España, septiembre 5-8.

Diccionario Collins (s. f.). Disponible en https://www.collinsdictionary.com/es/

El Tiempo (14 de junio 2017). *Estas son las compañías más grandes que operan en Colombia. El Tiempo*. Recuperado de https://www.eltiempo.com/economia/empresas/10-empresas-mas-grandes-de-colombia-98992

Entrepreneur (2018). *Qué es una startup.* Recuperado de https://www.entrepreneur.com/article/304376

European Commission (2017). *Proposal for an ePrivacy Regulation.* Recuperado de https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

Federal Trade Commission (2016). *FTC Issues Warning Letters to App Developers Using "Silverpush" Code.* Recuperado de https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpushcode

Federal Trade Commission (2017). *Cross-Device Tracking: An FTC Staff Report.* Recuperado de https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

Ferguson, A. G. (2017). *The Rise of Big Data Policing. Surveillance, Race and the Future of Law Enforcement.* New York: New York University Press.

Forbes (2012). *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.* Recuperado de https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#51a9aa7c6668

Forbrukerradet (2018). *Deceived by design. How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Recuperado de https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Irish Tech News (2018). *Interview with the European Data Protection Supervisor Giovanni Buttarelli: The GDPR is a radical update of the rule book for the digital age*. Recuperado de https://irishtechnews.ie/interview-with-the-european-data-protection-supervisor-giovanni-buttarelli-the-gdpr-is-a-radical-update-of-the-rule-book-for-the-digital-age/

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

Haupt, M. (2016). "Data is the New Oil"—A Ludicrous Proposition. Recuperado de https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294

INNpulsa Colombia (s. f.). Las mejores *start-ups* colombianas para invertir. Recuperado de https://www.innpulsacolombia.com/sites/default/files/civico_0.pdf

Kay, M., Matuszek, C. y Munson, S. A. (2015). *Unequal Representation and Gender Stereotypes in Image Search Results for Occupations.* Documento presentado en la Conferencia sobre Factores Humanos en Sistemas Informáticos (CHI), Seúl, República de Corea, abril 18-23.

La República (2018). Ingresos del top 10 de las compañías de telecomunicaciones sumaron $28 billones. *La República*. Recuperado de https://www.larepublica.co/especiales/las-empresas-mas-grandes-de-2017/ingresos-del-top-10-de-las-companias-de-telecomunicaciones-sumaron-28-billones-2728972

McDonald, A. M. (2018). *Statement of Aleecia M. McDonald, PhD Assistant Professor of the Practice, Information Networking Institute, Carnegie Mellon University Member of the Board of Directors, Privacy Rights Clearinghouse. California Assembly Committee on Privacy and Consumer Protection.* The California Consumer Privacy Act of 2018. Recuperado de http://www.archive.ece.cmu.edu/~ece734/readings/CA-Assembly-June26-2018-McDonald-testimony.pdf

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. y Hung Byers, A. (2011). *Big data: The next frontier for innovation, competition, and productivity.* New York: McKinsey Global Institute.

Mayer-Schönberger, V. y Cukier, K. (2013). *Big Data. A revolution that will transform how we live, work and think*. New York: Mariner Books.

McNeil, J. (s. f.). Big Brother's Blind Spot. Mining the failures of surveillance tech. *The Baffler*. Recuperado de https://thebaffler.com/salvos/big-brothers-blind-spot-mcneil

Noyb (2018). *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook.* Recuperado de https://noyb.eu/?lang=es%2F%3Flang%3Des

OEA (2015). *Informe del Comité Jurídico Interamericano. Privacidad y protección de datos personales.* 86º Periodo Ordinario de Sesiones. CJI/doc. 474/15 rev.2 adoptado el 26 de marzo de 2015.

Parmar, R., Mackenzie, I., Cohn, D., Gann, D. (2014). The new patterns of innovation. *Harvard Business Review*.

Portafolio (2017). Éxito y Zara, los líderes en *"retail"*. *Portafolio*. Recuperado de http://www.portafolio.co/negocios/empresas/empresa-lideres-en-retail-en-colombia-510250

Red Iberoamericana de Protección de Datos (2006). *Autorregulación y protección de datos personales.* Documento elaborado por el Grupo de Trabajo reunido en Santa Cruz de la Sierra, Bolivia, 3-5 de mayo.

Restrepo, M. A. (2009). Derecho administrativo contemporáneo: ¿derecho administrativo neopolicial? En *Retos y perspectivas de derecho administrativo. Segunda parte*. Bogotá: Editorial Universidad del Rosario.

Schneir, B. (2015). *Data and Golliath. The Hidden Battles to collect your data and control your world.* New York: Norton & Company.

Search Data Center (s. f). *Definition Política de Privacidad.* Recuperado de https://searchdatacenter.techtarget.com/es/definicion/Politica-de-privacidad

Serrato, J. K., Cwalina, C., Rudawski, A., Coughlin, T. y Fardelmann, K. (2018). US states pass data protection laws on the heels of the GDPR. *Data Protection Report.* Recuperado de https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/

Statista (2018a). *Number of internet users in Latin America from 2014 to 2019 (in millions).* Recuperado de https://www.statista.com/statistics/274860/number-of-internet-users-in-latin-america/

Statista (2018b). *Share of desktop search traffic originating from Google in Latin America in August 2017, by country.* Recuperado de https://www.statista.com/statistics/639072/googles-share-of-search-market-in-selected-countries-latam/

Statista (2018c). *Number of Facebook users in Latin America from 2014 to 2019 (in millions).* Recuperado de https://www.statista.com/statistics/282350/number-of-facebook-users-in-latin-america/

Statista (2018d). *Number of digital buyers in Latin America from 2014 to 2019 (in millions).* Recuperado de https://www.statista.com/statistics/251657/number-of-digital-buyers-in-latin-america/

Superintendencia de Industria y Comercio (s. f.). *Guía para la implementación del principio de responsabilidad demostrada* (*Accountability*). Recuperado de http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada

Superintendencia de Industria y Comercio (2014a). Resolución 36863 del 30 de mayo de 2014, "Por la cual se impone una sanción y se imparten unas órdenes". Recuperado de http://www.sic.gov.co/sites/default/files/files/Res%20No_%2036863%20de%202014%20-%20ALMACENES%20EXITO.pdf

Superintendencia de Industria y Comercio de Colombia (2014b). Concepto 14-218349-00003-0000 del 24 de noviembre de 2014.

Superintendencia de Industria y Comercio de Colombia (2016a). Concepto 14-218349-4-0, del 3 de marzo de 2016.

Superintendencia de Industria y Comercio de Colombia (2016b). Concepto 16-172268-00001-0000 del 9 de agosto de 2016.

Superintendencia de Industria y Comercio (2016c). Resolución 85568 del 13 de diciembre de 2016, "Por la cual se impone una sanción". Recuperado de http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE85568-2016.pdf

Superintendencia de Industria y Comercio (2017). Resolución 78911 del 30 de noviembre de 2017, "Por la cual se impone una sanción". Recuperado de http://www.sic.gov.co/sites/default/files/files/Normativa/Resoluciones/Resolucion_78911_2017.pdf

Superintendencia de Industria y Comercio (2018a). Resolución 44026 del 25 de junio de 2018, "Por la cual se impone una sanción administrativa". Recuperado de http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE44026-2018.pdf

Superintendencia de Industria y Comercio (2018b). Sanciones de protección de datos personales. Recuperado de http://www.sic.gov.co/sanciones-2018

Team Startup Colombia (2017). ¿Qué es? Recuperado de http://micrositios.mintic.gov.co/team-startup/

Terms Feed (2018). *Privacy Policies vs. Terms and Conditions*. Recuperado de https://termsfeed.com/blog/privacy-policies-vs-terms-conditions/#A_single_agreement_or_separate

The Guardian (11 de julio de 2018). *Facebook fined for data breaches in Cambridge Analytica scandal.* Recuperado de: https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

TICbeat (2017). Diccionario para saber todo sobre datos en la era digital. Recuperado de http://www.ticbeat.com/tecnologias/diccionario-para-saber-todo-sobre-datos-en-la-era-digital/

Tribunal de Justicia de la Unión Europea (2014). Caso Google Spain, S.L., y Google Inc., *vs*. Agencia Española de Protección de Datos y Costeja González, 13 de mayo de 2014.

World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class.* Recuperado de http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

ANEXO 1
Políticas de Privacidad consultadas

Alibaba Group. Privacy Policy. Última actualización: 24 de mayo de 2018. Recuperado de http://rule.alibaba.com/rule/detail/2034.htm

Almacenes Éxito S.A. *Política manejo de información y datos personales de Almacenes Éxito S.A.* Última actualización: febrero de 2014. Recuperado de https://www.grupoexito.com.co/files/Poltica_manejo_de_informacin_y_datos_personales_3.pdf

Amazon Inc. *Aviso de Privacidad.* Última actualización: 29 de agosto de 2017. Recuperado de https://www.amazon.com/gp/help/customer/display.html?language=es_US&nodeId=468496

Apple Inc. *Política de privacidad.* Última actualización: 22 de mayo de 2018. Recuperado de https://www.apple.com/legal/privacy/es-la/

Acsendo S.A.S. *Política de protección de datos personales*. Última actualización: 30 de junio de 2017. Recuperado de https://www.acsendo.com/es/privacidad/

Bending Spoons S.p.A. *Privacy Policy.* Sin fecha de última actualización. Recuperado de https://bendingspoons.com/privacy.html

Biko Development Inc. *Privacy Policy.* Sin fecha de última actualización. Recuperado de https://bikoapp.com/policy.html

Cívico Digital S.A.S. *Políticas de tratamiento de datos personales.* Última actualización: 7 de diciembre de 2017. Recuperado de https://www.civico.com/politicas-de-privacidad

Deezer SA. *Política de privacidad y cookies.* Sin fecha de última actualización. Recuperado de https://www.deezer.com/legal/personal-datas

Duety S.A.S. *Legal.* Última actualización: 14 de febrero de 2018. Recuperado de https://blog.duety.co/legal/#privacidad

Easy Taxi Colombia S.A.S. *Aviso de Privacidad*. Sin fecha de última actualización. Recuperado de http://www.easytaxi.com/co/terms-conditions/aviso-de-privacidad/

Facebook Inc. *Política de datos.* Última actualización: 19 de abril de 2018. Recuperado de https://www.facebook.com/privacy/explanation

Facebook Inc. *Política de privacidad de WhatsApp*. Última actualización: 24 de abril de 2018. Recuperado de 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.* Sin fecha de última actualización. Recuperado de http://www.fluvip.com/home_policy_for_the_protection?locale=es_CO

Google LLC. *Política de privacidad de Google.* Última actualización: 25 de mayo de 2018. Recuperado de 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.* Sin fecha de última actualización. Recuperado de 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").* Última actualización: 27 de febrero de 2018. Recuperado de https://domicilios.com/pages/politica-de-privacidad.html

IoT Services Inc. *Privacy Policy.* Sin fecha de última actualización. Recuperado de https://ubidots.com/privacy-policy/

Match Group, LLC. *Nuestro compromiso con usted.* Última actualización: 25 de mayo de 2018. Recuperado de https://www.gotinder.com/privacy?locale=es

Microsoft Corporation. *Declaración de privacidad de Microsoft.* Última actualización: agosto de 2018. Recuperado de https://privacy.microsoft.com/es-mx/privacystatement#mainhowtoaccesscontrolyourdatamodule

Microsoft Corporation. *Política de privacidad LinkedIn.* Última actualización: 8 de mayo de 2018. Recuperado de https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv

Netflix International B.V. *Declaración de privacidad.* Última actualización: 11 de mayo de 2018. Recuperado de https://help.netflix.com/legal/privacy

Rappi S.A.S. *Aviso de privacidad.* Sin fecha de última actualización. Recuperado de http://wordpress.rappi.com.br/terms-conditions/

Seguros Generales Suramericana S.A. *Política de privacidad y tratamiento de datos personales.* Última actualización: 16 de junio de 2017. Recuperado de https://www.segurossura.com.co/Paginas/legal/politica-privacidad-datos.aspx

SIA Joom (Latvia). *Joom Privacy Policy.* Sin fecha de última actualización. Recuperado de https://www.joom.com/es/privacy

Spotify AB. *Política de privacidad de Spotify*. Última actualización: 25 de mayo de 2018. Recuperado de https://www.spotify.com/co/legal/privacy-policy/

Telmex Colombia S.A. Política de tratamiento de la información. Última actualización: 26 de julio de 2013. Recuperado de https://www.claro.com.

co/portal/recursos/co/legal-regulatorio/pdf/Politicas_Seguridad_Inf_Claro.pdf

Uber B.V. *Política de privacidad.* Última actualización: 25 de mayo de 2018. Recuperado de https://privacy.uber.com/policy

Urbanite Inc. *Privacy Policy.* Sin fecha de última actualización. Recuperado de https://8fit.com/privacy/

Unilever N.V. *Aviso de privacidad*. Sin fecha de última actualización. Recuperado de https://www.unileverprivacypolicy.com/spanish/policy.aspx

Waze Mobile Limited. *Waze – Privacy Policy.* Última actualización: 25 de mayo de 2018. Recuperado de https://www.waze.com/es-419/legal/privacy

1DOC3 S.A.S. *Manual de políticas y procedimientos para la protección y tratamiento de datos personales.* Última actualización: 1 de marzo de 2014. Recuperado de https://www.1doc3.com/web/politicas

ANEXO 2
Clases de modelos de negocio basados en datos

Dimensión	Clases de modelos de negocio basados en datos		
Fuentes de datos	*Fuentes internas*	Datos ya existentes en la EMNBD	
		Datos generados por medio de monitoreo	Web tracking
			Sensores
			Crowdsourcing
	Fuentes externas	Datos proporcionados por el cliente	
		Datos proporcionados por socios estratégicos	
		Datos adquiridos	
		Datos que se pueden encontrar libremente en Internet	Open data
			Redes sociales
			Web crawling
Actividades clave	*Agregación*		
	Análisis	Descriptivo	
		Predictivo	
		Prescriptivo	
	Distribución		
	Visualización		
Segmento de clientes	*Business to Consumer (B2C)*		
	Business to Business (B2B)		
	Business to Consumer to Business (B2C2B)		
Propuesta de valor	*Datos*		
	Información y conocimiento		
	Bienes y servicios no digitalizados		
	Bienes y servicios mejorados		
	Activos físicos digitalizados		
	Combinación de datos		
	Comercialización de datos		
	Codificación de procesos		

Dimensión	Clases de modelos de negocio basados en datos		
Modelo de generación de ingresos	*Publicidad*		
	Venta		
	Arriendo/Préstamo		
	Licenciamiento		
	Freemium		
	Cobro por uso		
	Precio por proyecto		
	Suscripción		
	Comisión		
Estructura de costos	*Esfuerzo para generar datos*		
	Datos generados como un subproducto de sus propias actividades		

FUENTE: elaboración propia a partir de Philipp Max Hartmann *et al.* (2014) y Myrla Alcaíno *et al.* (2015).

ANEXO 3
Asistentes al grupo focal realizado el 20 de noviembre de 2018 en las instalaciones de Dejusticia

	Entidad	Representante
1	Fundación Karisma	Juan Diego Castañeda
2	Linterna Verde	Carlos Cortés
3	Consejo Privado de Competitividad	Lorena Lizarazo
4	Universidad Externado de Colombia	Camilo de la Cruz
5	Universidad Externado de Colombia	Daniel Castaño
6	Universidad del Rosario	Grenfieth Sierra
7	Ex Superintendente Delegado para la Protección de Datos Personales (2012-2015)	José Alejandro Bermúdez
8	Corte Suprema de Justicia	Ana Carolina molina
9	Consultora de UNICEF en Big Data	Viviana Cañón
10	Privacy International	Aillidh Callander (vía Bluejeans)
11	Omidyar	Gabriela Hadid (vía Bluejeans)
12	Dejusticia	Vivian Newman
13		María Paula Ángel
14		Laura Guerrero
15		Celso Bessa
16		Sophie Kushen

Adicionalmente, al grupo focal fueron también invitados representantes de las siguientes entidades del Estado, academia, sociedad civil y empresas, quienes sin embargo no asistieron: Superintendencia Delegada para la Protección de Datos Personales, Dirección de Desarrollo de Industria TI del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), Despacho del magistrado Fernando Reyes Cuartas (magistrado ponente del Auto 285/18), Centro de Internet y Sociedad de la Universidad del Rosario, Grupo de Estudios en Internet, Comercio electrónico, Telecomunicaciones e Informática (Gecti) de la Universidad de los Andes, Centro de Investigación en Derecho Informático y de las Nuevas Tecnologías de la Universidad Externado de Colombia, Decanatura de Derecho de la Universidad de los Andes, Fundación para la Libertad de Prensa (FLIP), Enter.co, Acessnow, Media Legal Defence Initiative, Tech & Law, Data&Tic, Microsoft Colombia, Facebook, Samsung, Rappi y Google Colombia. En el caso de esta última empresa pudimos tener una videoconferencia en la que nos manifestaron su interés de enviar sus

comentarios al documento. Sin embargo, a la fecha no hemos recibido ninguna comunicación al respecto.

VOLVER A TABLA DE CONTENIDO

ANEXO 4

Aplicaciones más descargadas en AppStore en los primeros cinco días de los meses de julio, agosto y septiembre de 2018

iPhone Top App Matrix										
1/07/18	DirectTV Sports	DirectTV	WhatsApp	Instagram	YouTube	Netflix	Deezer	Tinder	LinkedIn	8fit
2/07/18	DirectTV Sports	DirectTV	WhatsApp	30 Days Fitness Challenge	Instagram	Netflix	Deezer	Tinder	Clash Royale	Candy Crush Saga
3/07/18	DirectTV Sports	DirectTV	WhatsApp	Messenger	Selección Colombia Oficial	Netflix	Deezer	Tinder	Dropbox	Clash Royale
4/07/18	WhatsApp	Messenger	Instagram	Facebook	YouTube	Netflix	MARVEL Contest of Champions	Deezer	Tinder	LinkedIn
5/07/18	WhatsApp	Instagram	Facebook	Messenger	YouTube	Netflix	Tinder	Deezer	Sniper 3D	MARVEL Contest of Champions
1/08/18	WhatsApp	Facebook	Messanger	Instagram	YouTube	Netflix	Deezer	Tinder	Candy rush Saga	Captain Tsubasa
2/08/18	WhatsApp	Messenger	Facebook	Instagram	YouTube	Netflix	Deezer	LinkedIn	Tinder	App removida
3/08/18	WhatsApp	Messenger	Facebook	Instagram	YouTube	Netflix	Deezer	Tinder	App removida	LinkedIn
4/08/18	WhatsApp	Facebook	Instagram	Messenger	YouTube	Netflix	Deezer	Tinder	LinkedIn	App removida
5/08/18	WhatsApp	YouTube	Facebook	Instagram	Messenger	Netflix	Tinder	Deezer	LinkedIn	Fortnite
1/09/18	Hello Star	WhatsApp	YouTube	Aliexpress	Messenger	Netflix	Tinder	Deezer	Luxy Millionaire	Candy Crush Saga
2/09/18	Hello Star	YouTube	WhatsApp	Facebook	Instagram	Netflix	Deezer	Tinder	LinkedIn	Summoners War
3/09/18	WhatsApp	Hello Star	Facebook	Messenger	YouTube	Netflix	Tinder	Deezer	Clash Royale	LinkedIn

4/09/18	WhatsApp	Facebook	Messanger	Instagram	YouTube	Netflix	Deezer	Tinder	LinkedIn	Clash Royale
5/09/18	WhatsApp	Facebook	Messanger	Instagram	YouTube	Netflix	Clash Royale	Deezer	Tinder	LinkedIn

VOLVER A TABLA DE CONTENIDO

ANEXO 5
Aplicaciones más descargadas en Google Play en los primeros cinco días de los meses de julio, agosto y septiembre de 2018

Google Play Top App Matrix										
1/07/18	WhatsApp	Messenger	Facebook Lite	Facebook	Instagram	Google Drive	Tinder	Lords Mobile	King of Avalon	Clash Royale
2/07/18	WhatsApp	Messenger	App removida	Facebook Lite	Facebook	Google Drive	Tinder	Lords Mobile	Clash Royale	Captain Tsubasa
3/07/18	WhatsApp	Messenger	App removida	Facebook Lite	Facebook	Google Drive	Tinder	Clash Royale	Lords Mobile	Captain Tsubasa
4/07/18	WhatsApp	Messenger	Facebook Lite	Rise Up	Instagram	Google Drive	Tinder	Clash Royale	Lords Mobile	Captain Tsubasa
5/07/18	WhatsApp	Messenger	Facebook Lite	Rise Up	Instagram	Google Drive	Tinder	Clash Royale	Lords Mobile	Captain Tsubasa
1/08/18	WhatsApp	Messenger	Facebook Lite	Facebook	Instagram	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
2/08/18	WhatsApp	Messenger	Facebook Lite	Facebook	Joom	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
3/08/18	WhatsApp	Messenger	Facebook Lite	Facebook	Messenger Lite	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
4/08/18	WhatsApp	Messenger	Facebook Lite	Facebook	Messenger Lite	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
5/08/18	WhatsApp	Messenger	Facebook Lite	Facebook	Instagram	Google Drive	Tinder	Lords Mobile	Garena Free Fire	Clash Royale
1/09/18	Hello Star	Aliexpress	WhatsApp	Facebook Lite	Messenger	Google Drive	Tinder	Lords Mobile	Garena Free Fire	Clash Royale

2/09/18	WhatsApp	Messenger	Facebook Lite	Hello Star	Facebook	Google Drive	Tinder	Lords Mobile	Garena Free Fire	Clash Royale
3/09/18	WhatsApp	Messenger	Hello Star	Facebook Lite	Facebook	Google Drive	Garena Free Fire	Tinder	Lords Mobile	Clash Royale
4/09/18	WhatsApp	Messenger	Hello Star	Facebook Lite	Facebook	Google Drive	Garena Free Fire	Tinder	Clash Royale	Lords Mobile
5/09/18	WhatsApp	Messenger	Facebook Lite	Hello Star	Facebook	Google Drive	Garena Free Fire	Clash Royale	Tinder	Lords Mobile

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

DOCUMENTOS 48

En el 2018 entró en vigencia el Reglamento General de Protección de Datos de la Unión Europea y se expidió la Ley de Privacidad del Consumidor del estado de California, que buscan equilibrar el desarrollo de la economía digital con la garantía de los derechos a la intimidad y a la protección de datos personales. ¿Cómo? Por medio de la regulación de nuevas fuentes de datos, tipos de tratamiento y finalidades de tratamiento que son propias de la era digital, y que incluyen el uso de cookies, el web crawling, los algoritmos, el profiling, la toma de decisiones automatizadas, la comercialización de datos y la publicidad comportamental. ¿Qué se ha hecho en Colombia para garantizar dichos derechos en el marco de la economía digital? En este documento exploramos el grado de preparación de nuestro régimen jurídico de protección de datos personales y de nuestras autoridades competentes para enfrentar los riesgos que la era digital plantea para distintos valores y derechos y hacer así rendir cuentas a las empresas con modelos de negocios basados en datos (EMNBD). Para ello, a partir de la revisión de sus políticas de privacidad analizamos la forma de operar de una muestra ilustrativa de 30 EMNBD, dentro de las que sobresalen por su poder económico, tecnológico y social los llamados GAFAM (Google, Apple, Facebook, Amazon y Microsoft).

978-958-5441-65-1

9 789585 441651