DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

LA EXPLOTACIÓN DE LOS DATOS PERSONALES POR LOS GIGANTES DE INTERNET

THE EXPLOITATION OF PERSONAL DATA BY INTERNET GIANTS

Ángela CUBILLOS VÉLEZ*

RESUMEN. En este artículo se examinan los diferentes aspectos de la protección de datos personales en Colombia que se inspira en el modelo europeo. Posteriormente, se analiza si la protección consagrada en la actual legislación resulta eficaz frente a la utilización de los datos personales por las grandes compañías prestadoras de servicios en internet, concretamente se estudia si las políticas de privacidad de los gigantes de internet protegen realmente los datos personales. Finalmente, se presentan las posibles soluciones para asegurar la protección efectiva de los datos personales empleados por estas empresas como base de su modelo de negocios.

PALABRAS CLAVE. *Habeas data*, protección de datos personales, privacidad, transferencia internacional de datos.

ABSTRACT. This article examines the different aspects of the protection of personal data in Colombia that is inspired by the European legal model. Later, the author analyses if the protection

* Abogada por la Universidad Externado de Colombia, DSU derecho civil Universidad Panthéon-Assas; máster en derecho de comercio electrónico y economía digital de la Universidad Panthéon-Sorbonne, y doctorante en la misma casa de estudios; investigadora en el Centro de Investigación en Derecho Informático (CIDI) de la Universidad Externado de Colombia, *angelac_86@hotmail.com*.

Fecha de recepción: 6 de junio de 2016.
Fecha de dictamen: 12 de septiembre de 2016.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

granted in the actual legislation results effective in the face of the use and management of personal data by the big companies that provide internet services, specifically she addresses whether the politics of privacy of the internet giants effectively protects personal data. Finally, the author presents the possible solutions to secure the protection of personal data used by the information technologies companies as the base of a business model.

KEY WORDS. Habeas data, personal data protection, privacy, international transference of data.

I. Introducción

En el mundo, el mercado digital está dominado hasta el presente por las grandes empresas del Silicon Valley, como Google,[1] Apple,[2] Facebook[3] y Amazon.[4] A ellas se les ha atribuido el nombre de *gigantes de internet*, en primer lugar, porque se encuentran en una situación de posición dominante dentro de diferentes mercados digitales; en segundo lugar, porque estas multinacionales poseen varios mercados conexos en internet[5] que subsisten gracias a la venta de publicidad, que constituye el mayor ingreso de estas empresas.[6] Ellas tienen importantes cantidades de usuarios,[7] lo que les permite actuar de manera autónoma e independiente con relación a la competencia.

[1] Google se encuentra en una situación de posición dominante en el mundo dentro del mercado pertinente de motores de búsqueda con el 88.66% (La Redacción de Journal Du Net, 2016).

[2] Apple, junto con Samsung, se encuentran en una situación de posición dominante en el mercado de teléfonos móviles (Neilime, 2015).

[3] Facebook reivindica alrededor de 1.6 millones de utilizadores mensuales en el mundo, con ganancias cercanas a los 18 millones de dólares para el 2015, que provienen de la publicidad dirigida (Prodhan Et Harro Ten Wolde, 2016).

[4] Amazon tiene el 40% del mercado de los libros nuevos en Estados Unidos; de igual forma, posee los dos tercios del mercado del libro electrónico, y sobre las ventas de libros en línea, la parte del mercado aumentaría a 75% (Rauline, 2015).

[5] Google cambió de nombre en agosto de 2015 convirtiéndose en Alphabet; este *holding* dividió sus servicios para dar una ilusión de transparencia como respuesta al proyecto de resolución del Parlamento Europeo, que proponía desmantelar los servicios de Google (Karayan, 2014).

[6] Google en el primer semestre de 2015 reportó ganancias de 17.3 millones de dólares, dentro de los cuales 15.5 millones de dólares provienen de la publicidad (Jaimes, 2015).

[7] Facebook es utilizado por más de una persona de cada siete (La Redacción de Diario Le Monde, 2012).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

Un problema persistente en materia de protección de datos personales es la comercialización o explotación económica de los datos de los que se allegan los gigantes de internet (Rochfeld, 2015: 91), que se promueven con una gratuidad aparente,[8] mediante la cual atraen a los usuarios, quienes ponen a su disposición información personal, sin conocer el alcance de la autorización del uso que hay de por medio. Una vez recolectados, estos datos son objeto de comercialización, de manera que se financia el acceso gratuito a sus servicios con la venta de los datos personales inscritos por los usuarios, que son utilizados posteriormente, por ejemplo, para ofrecer publicidad dirigida y personalizada.

Para resolver la anterior problemática de la comercialización de datos se intentarán solucionar las siguientes preguntas: ¿las políticas de privacidad de los gigantes de internet protegen realmente los datos personales de acuerdo con la reglamentación existente en Colombia?, y ¿la utilización de los datos personales por los gigantes de internet se encuentra en conformidad con las disposiciones vigentes sobre protección de datos personales?

Con el fin de abordar las problemáticas planteadas, se examinará, en primer lugar, la protección actual de los datos personales explotados por los gigantes de internet en Colombia, y a manera de proposición, en la segunda parte se analizarán cuáles son los avances indispensables para asegurar la protección efectiva de los datos personales frente a la utilización de los mismos por los gigantes de internet.

II. La protección actual de los datos personales explotados por los gigantes de internet en Colombia

Dentro del presente acápite se presentarán los avances jurídicos relevantes sobre protección de datos personales en Colombia (1), y en un segundo tiempo se examinará cómo a pesar de dichos avances las problemáticas persisten cuando se trata de la comercialización de los datos realizada por los gigantes de internet (2).

1. *Los avances jurídicos relevantes en materia de protección de datos en Colombia*

La protección de datos personales en Colombia es el producto de una evolución jurídica esperada desde su consagración constitucional en 1991

[8] Esta gratuidad resulta interesante para los usuarios, pero como es bien sabido, "si es gratuito somos nosotros el producto".

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

(Remolina, 2015: 120), y su materialización legislativa tiene lugar posteriormente en 2008 y 2012. Colombia ha acogido el modelo de la Directiva 95/46/CE (1995), aplicable en Europa hasta el 2018, año en el cual entrará en vigor el reglamento relativo a la protección de datos personales que se deriva de la adopción el 14 de abril de 2016 por el Parlamento Europeo (Reglamento 2016/679).

Los avances más relevantes sobre protección de datos personales en Colombia se presentan en tres momentos. El primero ocurre en 1991 con el reconocimiento constitucional de la protección de datos personales (artículo 15, Constitución Política de Colombia) —Colombia es uno de los doce países de América Latina que ha elevado a nivel constitucional esta protección—.[9] El segundo avance se da con la adopción de una reglamentación sectorial, la Ley Estatutaria Núm. 1266 de 2008, que brinda una protección restrictiva para los datos comerciales y financieros. Finalmente, en un tercer tiempo se adoptó la Ley Estatutaria Núm. 1581 de 2012 y su anhelada reglamentación general por el Decreto 1377 de 2013.

Es menester precisar que en Colombia existe una reglamentación híbrida (sentencia C-748/11), ya que la ley de regulación sectorial de 2008 (o Estatutaria Núm. 1266) debe articularse con la ley general de 2012 (o Estatutaria Núm. 1581), toda vez que la primera no cumple con las exigencias de una regulación general de protección de datos (Remolina, 2015: 136). A modo de ilustración, la Ley no incluye los datos sensibles dentro del articulado; omite fijar el alcance y las exigencias del contenido del consentimiento y el régimen de transferencia internacional de datos, puntos fundamentales que deben estar presentes en cualquier legislación que regule la materia, dado que el consentimiento es una condición *sine qua non* para el tratamiento de datos, y las grandes compañías ofrecen servicios en internet y alojan los datos de los ciudadanos colombianos fuera del territorio nacional.

La Ley de 2012 llena los vacíos de la anterior regulación de 2008; actualmente, Colombia cuenta con niveles jurídicos adecuados de protección, en lo que concierne a su positivización. La Ley consagra los principios generales que rigen el tratamiento de datos personales (artículo 4o. del Decreto 1377 de 2013), dentro de los cuales es importante citar para

[9] El artículo 15 de la Constitución Política de Colombia (1991) señala: "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases 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…".

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

el caso del tratamiento de datos personales por los gigantes de internet, los siguientes:

1) El principio de libertad, que se encuentra ligado a la importancia del consentimiento informado, expreso y previo del titular. La delimitación de la autorización establece el marco dentro del cual es posible efectuar un tratamiento de datos (Remolina, 2015: 132) por las grandes compañías de internet.
2) El principio de acceso y de la circulación restringida, que establece que el tratamiento deberá ser realizado únicamente por las personas autorizadas por el titular. A pesar de la existencia de este principio, la dificultad reside en el control de la circulación y el acceso a los datos, en especial si se tiene en cuenta el volumen de datos almacenados por los gigantes de internet.
3) El principio de transparencia, por su parte, otorga al titular el derecho de acceder a la información que le concierne ante el responsable del tratamiento en cualquier momento. Es importante señalar que cuando se trata de información que poseen los gigantes de internet, el usuario puede desconocer que sus datos están siendo objeto de un tratamiento, piénsese en el caso de recolección de una dirección IP, de la instalación de una *cookie* o de las palabras claves introducidas dentro de un motor de búsqueda.
4) Por otra parte, la Ley consagra el principio de seguridad y de neutralidad tecnológica, donde la información debe ser asegurada y manejada con las medidas necesarias para prevenir el uso o acceso no autorizado. En este mismo sentido se consagró el principio de confidencialidad, que deberá ser respetado, incluso, de forma posterior al tratamiento de los datos, salvo si se trata de datos de naturaleza pública.
5) En igual sentido, el tratamiento de datos personales debe ser limitado a un término razonable y necesario de utilización, recopilación, almacenamiento y difusión de datos personales de acuerdo con los fines que justifiquen el tratamiento, en virtud del principio de la limitación en el tiempo del tratamiento de datos personales reconocido por el Decreto reglamentario (artículo 11 del Decreto 1377 de 2013).
6) Finalmente, un principio de vital importancia para el tema que nos ocupa es el principio de la exigencia de normas de protección iguales para la transferencia internacional de datos (Sentencia C-748/11). Este principio reconocido por vía jurisprudencial es

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

fundamental, toda vez que la explotación de los datos realizada por los gigantes de internet se efectúa fuera del territorio.

Ahora bien, dentro de los avances más relevantes en materia de protección de datos personales en Colombia encontramos que la legislación de 2012 contiene las definiciones de los términos esenciales. La Ley define de manera amplia un dato personal como "toda información vinculada o que puede ser asociada a una o varias personas naturales determinadas o determinables" (artículo 3o., C, de la Ley Estatutaria Núm. 1581 de 2012). En este orden de ideas, es posible proteger un mayor número de datos asociados a una persona natural, toda vez que el titular puede ser determinable, de manera que poca información quedará excluida del concepto de dato personal. Por ejemplo: una dirección IP o una *cookie* que ha instalado un gigante de internet en el computador de una persona permite identificar al titular de la información; en este caso estamos frente a un dato personal.

El tratamiento, a su vez, es definido como toda operación o conjunto de operaciones sobre los datos personales, como la recolección, el almacenamiento, la utilización, la circulación o la supresión (artículo 3o., G, Ley Estatutaria Núm. 1581). Es posible observar que la definición no excluye los tratamientos no automatizados del campo de aplicación de la Ley.

Con lo relacionado al titular de los datos, es importante precisar que las personas jurídicas pueden igualmente ejercer acciones para proteger su derecho de *habeas data* en virtud de un reconocimiento jurisprudencial (sentencia T-462/97). Es criticable que la Ley no haya previsto expresamente la protección para las personas jurídicas, toda vez que los datos adquiridos en el giro ordinario de su negocio deberían ser preservados, esto con el fin de impedir que se presenten casos de competencia desleal y el abuso de posición dominante cuando otras compañías hacen uso de dichos datos. A manera de ilustración, el comportamiento de Google influencia la oferta y la demanda en el mercado digital; Google tiene acceso a una gran cantidad de información de la concurrencia y a los nuevos avances tecnológicos (sentencia Google France, Google Inc. / Bottin Cartographes, 2013).

De igual forma, la Ley define al encargado del tratamiento como una "persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento" (artículo 3o., D, Ley Estatutaria Núm. 1581). El responsable del tratamiento, por su parte, es definido como "toda persona natural o jurídica, pública o privada, que efectúa el tratamiento de datos personales por el mismo o en asociación con otras personas, actuando a

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

nombre y por la cuenta del responsable del tratamiento" (artículo 3o., E, Ley Estatutaria Núm. 1581).

Ahora bien, en materia de responsabilidad, a pesar de no encontrarse previsto en la Ley, el contrato que concluya el encargado del tratamiento con el responsable del tratamiento debería estipular la repartición de obligaciones de seguridad y confidencialidad; en principio, el encargado del tratamiento no podrá actuar sino por instrucción expresa del responsable del tratamiento. A medida que las instrucciones otorgadas al encargado del tratamiento sean más amplias, mayor será el riesgo para este último de comprometer su responsabilidad. Por el contrario, si los datos se utilizan, por ejemplo, con el fin de realizar una prospección comercial no prevista dentro del contrato suscrito con el responsable del tratamiento, estaríamos frente a una finalidad diferente que obligaría al encargado del tratamiento.

Por otra parte, un tema de vital importancia es la "aplicación territorial de la Ley", pues el legislador no exige que el responsable del tratamiento se encuentre establecido en Colombia,[10] y con esta disposición se pretende evitar (en teoría) la deslocalización masiva de datos. De manera que la utilización de computadores, de terminales o de servidores en el territorio colombiano constituye un tratamiento de datos. La Ley no contempla ninguna excepción, de ahí que el simple tránsito de datos deberá respetar la legislación.

Grandes compañías de Silicon Valley sostienen que el tratamiento de datos se efectúa en Estados Unidos, porque los servidores se encuentran en territorio americano; con este argumento se ha pretendido eludir la aplicación de la Ley, sosteniendo que no están domiciliados físicamente en el país (Remolina, 2015). Otro argumento utilizado es que el tratamiento se realiza de manera involuntaria (Rochfeld, 2015: 94). Sin embargo, estas compañías realizan un tratamiento de datos en Colombia, prueba de lo anterior: ellas instalan *cookies* en el territorio colombiano.

En este sentido, la jurisprudencia europea de la Corte de Justicia de la Unión Europea (CJUE), "sentencia del caso C-131/12", es de vital importancia,[11] toda vez que reconoce por primera vez que Google no podrá continuar argumentando que no realiza un tratamiento de datos personales dentro del territorio europeo; la CJUE, en el caso de origen español,

[10] El artículo 2o. de la Ley Estatutaria Núm. 1581 de 2012 señala que hay tratamiento de datos personales en Colombia cuando "existe utilización de los medios de tratamiento en el territorio".

[11] La CJUE considera, en este caso, que el operador de un motor de búsqueda definía bien a través del algoritmo implementado y de la creación y organización de los hipervínculos, los medios y las finalidades del tratamiento.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

es clara al considerar que este motor de búsqueda es un responsable del tratamiento (Rochfeld, 2015: 91). La autoridad colombiana encargada de la protección de datos ya comparte esta misma posición (Resolución núm. 4046), de manera que existe un avance importante en la materia.

Otro tema central es el consentimiento previo del titular de los datos (Remolina, 2015: 133), que permite al titular decidir cómo desea proteger su vida privada y reputación. Dentro de las condiciones de licitud del tratamiento de datos personales, el consentimiento constituye el punto central para determinar si ha existido o no violación.

La ley colombiana reconoce la importancia de la manifestación de la voluntad del titular de los datos. Para que las condiciones de licitud del tratamiento sean respetadas es indispensable la autorización del titular de la información, quien deberá expresar su "consentimiento previo, expreso e informado" (artículo 2o., a, Ley Estatutaria Núm. 1581). La ley colombiana prohíbe toda autorización tácita; el silencio no es considerado como una forma de otorgar el consentimiento, además de que no debe existir coacción en la manifestación de la voluntad, que tendrá que ser clara, precisa e ininteligible. Así, por ejemplo, la casilla preseleccionada para aceptación o la redacción ambigua de políticas de privacidad o de condiciones generales de utilización vician el consentimiento del titular y deberán ser consideradas como actos ilícitos. El consentimiento tendrá que ser registrado en un medio que permita su consulta posterior, y la carga de la prueba pesa sobre el responsable del tratamiento.

En igual sentido, el titular tiene la facultad de revocar la autorización, y solicitar al responsable del tratamiento o al encargado la supresión de los datos personales en todo momento (artículo 9o., Decreto 1377 de 2013). El "derecho al olvido" de acuerdo con la legislación colombiana no existe como disposición expresa; sin embargo, hay un derecho a la supresión de datos (artículo 8o., Ley Estatutaria Núm. 1581 de 2012). Si los datos no son suprimidos por el responsable, el titular podrá solicitar a la autoridad pública encargada de la protección de los datos personales, la supresión de los datos y/o la revocación de la autorización. En derecho comparado, varias legislaciones han reconocido el derecho al olvido: el primer caso se dio en 2014 con la jurisprudencia de la CJUE del caso Google-España (sentencia del caso C-131/12), y el segundo, con la decisión del 10 de octubre de 2014 del Tribunal de Tokio, en la cual se le ordenó a Google la supresión de un centenar de links hacia páginas que afectaban los datos personales de un titular concernientes a un crimen que no había cometido (La Redacción de la Tribune, 2014).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

La legislación colombiana incluye, igualmente, condiciones específicas de licitud en materia de "datos sensibles"[12] y de protección de menores. Por ejemplo, existe una protección especial para los datos biométricos[13] y aquellos que conciernen la salud o la vida sexual. Ninguna actividad puede ser subordinada a la autorización del titular para suministrar datos personales sensibles (artículo 6o., Decreto 1377 de 2013).

Una vez examinado el campo de aplicación de la ley, es posible afirmar que el marco jurídico existente en Colombia consagra los elementos indispensables para efectuar un control material sobre protección de datos personales, toda vez que la Ley de 2012 permite:

1) Determinar si existe o no un dato personal. Por ejemplo, en el caso de tratamiento de datos para fines estadísticos, la Ley permite inferir que no se trata de un dato personal cuando no sea posible determinar quién es el titular de la información, porque es necesario asociar la información a la persona.
2) Establecer si existe un tratamiento de datos personales, sea éste automatizado o no.
3) Identificar quién es el responsable del tratamiento y, en el eventual caso, quién es el encargado del tratamiento.
4) Analizar si se cumplen las exigencias de la aplicación territorial.
5) Examinar si se respetan las condiciones de licitud del tratamiento de las bases de datos personales. Con la legislación vigente es posible determinar si la recopilación de datos es leal, lícita, transparente, y si las finalidades del tratamiento están precisadas de forma explícita. De igual manera, es posible saber si el tratamiento de datos personales es proporcional, adecuado y pertinente. Gracias a la reglamentación existente es posible ejercer un control sobre la calidad del almacenamiento de los datos para conocer si éstos son exactos, completos y actualizados; igualmente, es posible estable-

[12] Los datos sensibles son todos aquellos que afectan la vida privada del titular, cuyo uso indebido puede generar discriminación, como aquellos que revelan el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la adhesión a sindicatos u organizaciones sociales, los derechos del hombre, los derechos y garantías de los partidos políticos de oposición, así como los datos que conciernen la salud, la vida sexual y los datos biométricos (artículo 5o., Ley Estatutaria Núm. 1581).

[13] La biometría es una palabra que proviene del griego *bio* (vida) y *metron* (medida); a través de esta disciplina es posible medir, analizar y, posteriormente, identificar cada individuo con el fin de conocer su identidad, gracias al uso de diferentes técnicas. Dentro de los parámetros biométricos se encuentran, entre otros, la huella digital, el iris del ojo, la identificación por voz, la identificación por los rasgos del rostro.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

cer si la duración de la conservación no excede el tiempo necesario de la finalidad para la cual se recopilaron los datos. Por último, dentro de las condiciones de licitud, la Ley otorga las herramientas para determinar si existe o no una manifestación de voluntad expresa, indiscutible, libre, específica e informada del titular.

6) Una vez establecido lo anterior, la Ley permite verificar si se han respetado las formalidades exigidas en la misma, especialmente si los derechos de los titulares de la información han sido respetados y si el responsable del tratamiento cumple con las obligaciones previstas.

7) De igual manera, la Ley prevé la aplicación de controles y sanciones, lo que podría crear un efecto disuasivo. Sin embargo, pese a este reconocimiento, la Ley de 2012 impone multas bajas, que para el caso de los gigantes de internet resultarían simbólicas. Ejemplo, una multa de 2,000 salarios mínimos en pesos colombianos (artículo 23, Ley Estatutaria Núm. 1581 de 2012) no afectaría el resultado del ejercicio de una empresa como Google que tiene ingresos que sobrepasan los 75 millones de dólares en el 2015 (Escande, 2016). En igual sentido, la suspensión temporal de actividades (artículo 23, Ley Estatutaria Núm. 1581 de 2012) se aplica únicamente por un término de seis meses, y la suspensión definitiva (artículo 23, Ley Estatutaria Núm. 1581 de 2012) opera sólo para los datos sensibles, con lo cual los demás datos personales no se benefician de esta sanción. De otra parte, las sanciones se aplican para personas de naturaleza privada (artículo 23, Ley Estatutaria Núm. 1581 de 2012), por lo que la competencia sancionatoria de la autoridad encargada de la protección de datos se ve restringida cuando se trata de personas jurídicas de naturaleza pública.

A pesar de los avances citados precedentemente, como se analizará a continuación, las problemáticas de violación de datos personales persisten cuando se trata de la comercialización de los datos realizada por los gigantes de internet.

2. *Las problemáticas persistentes en materia de protección de datos por la comercialización que realizan los gigantes de internet*

La ineficacia de la regulación actual obedece en gran parte a la comercialización de los datos realizada por los gigantes de internet. Empresas

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

como Facebook, Google o Apple proponen un servicio gratuito al internauta; sin embargo, detrás de esta gratuidad se esconde una finalidad económica. De manera que la gratuidad sólo es aparente y la audiencia, es decir, el titular de los datos personales, será conducido sutilmente a no darse cuenta del consentimiento otorgado.

Dentro del modelo económico de gratuidad se encuentra la estructura de la lógica interagente, que es el gran invento de la economía industrial de 2000, creado por el Premio Nobel de Economía, el francés Jean Tirole (Tirole, 1993). Este modelo de mercado se denomina mercado bilateral o de dos fases (en francés *marché biface*). Un mercado de dos fases es un mercado en el cual existen dos tipos de consumidores diferentes, pero interdependientes entre sí.

Con el fin de explicar la comercialización de los datos realizada por los gigantes de internet, el modelo de Google ilustra bien la gratuidad en un mercado de dos fases. Por una parte, Google propone una serie de servicios gratuitos a los internautas, quienes confían sus datos personales a esta empresa, y por otra, Google monetiza la audiencia gracias a la venta de espacios publicitarios basados en los datos de los internautas y en la instalación de *cookies* para orientar los resultados. De esta manera, el modelo de gratuidad es doblemente aparente, porque Google genera ingresos con los datos personales de los internautas y con la publicidad.

En este mercado de dos fases existe un equilibrio económico, toda vez que convergen tres condiciones: la primera, los gigantes de internet poseen dos tipos de clientela; en segundo lugar, los beneficios de los clientes de un grupo aumentan con el número de clientes del otro grupo, de ahí la existencia de la interdependencia, y, finalmente, hay una plataforma intermediaria.

En un inicio, estas compañías utilizaban los datos para realizar prospección comercial; no obstante, las finalidades del tratamiento cambiaron y hoy en día estos datos se emplean para efectuar orientación personalizada de la publicidad a cada usuario. Ejemplo, si un internauta busca un tiquete de avión, la publicidad que va a encontrar posteriormente cuando realiza la navegación va a ser dirigida sobre el tema de la búsqueda realizada con anterioridad, a esto se le denomina publicidad orientada o dirigida.

La venta de esos espacios publicitarios sucede en cuestión de segundos; esto se realiza con base en las visitas que hacemos diariamente a los sitios de internet. Aquí vale la pena preguntarse si el tratamiento de estos datos respeta la protección de los datos personales. Sobre este asunto, la gran mayoría de utilizadores coincidirá en afirmar que nunca han consentido, al menos de manera clara, expresa, informada y consciente, sobre la

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

autorización de una publicidad dirigida en sus visitas realizadas a los diferentes sitios. En este orden de ideas, los tratamientos de datos personales efectuados por los gigantes de internet no se encuentran conformes a la legislación colombiana vigente, toda vez que no respetan las condiciones de licitud del tratamiento.

Los gigantes de internet han logrado realizar el trabajo que antiguamente hacía el departamento de *marketing* de una empresa: ellos conocen el receptor del mensaje y esto les permite dirigir la publicidad a cada usuario. Ésta es una de las principales razones por las cuales los actores de internet temen a un sistema de protección de datos personales demasiado garantista, porque, como ya se mencionó, la mayoría de los ingresos de estos gigantes provienen de esta actividad.

Otra problemática existente en materia de datos personales consiste en la orientación publicitaria efectuada con el uso de las *cookies*. Las *cookies* son informaciones instaladas en el disco duro del computador por el servidor del sitio que visita el titular de la información; ellas contienen el nombre del servidor que la deposita, una identificación con un número único y eventualmente con una fecha de expiración (CNIL, s.a.).

La instalación de *cookies* constituye un tratamiento de datos personales, toda vez que estas informaciones permiten identificar al titular de la información. La cantidad de *cookies* que se instalan durante la navegación en internet es considerable. Existen varias *cookies* que no cumplen con todas las exigencias de un consentimiento libre, expreso e informado. Otras se contentan con informar al titular que se instalarán *cookies* mediante una ventana emergente, condicionando la navegación a la aceptación de su instalación.[14] Estas ventanas emergentes no permiten rechazar la instalación de *cookies* y se cierran inmediatamente. Ninguna actividad en internet debería ser subordinada a la autorización del titular para suministrar datos personales. En este sentido, la Ley de protección de datos personales de Colombia es clara en exigir un consentimiento libre; sin embargo, hasta la fecha no se han impuesto sanciones por este tipo de comportamientos.

Igualmente, los gigantes de internet emplean los datos que dejamos en nuestro paso por la red para realizar la identificación del titular a partir de los datos biométricos, analizando las características biológicas, como la identificación a través de la voz o de los rasgos del rostro de las fotos que

[14] Por ejemplo, en un sitio de internet puede aparecer un *pop-up* o ventana emergente que informa al titular de la siguiente forma: "utilizamos *cookies* propias y de terceros para mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias mediante el análisis de sus hábitos de navegación. Si continúa navegando, consideramos que acepta su uso".

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

dejamos en las redes sociales, como Facebook. Asimismo, estos datos son vendidos a las compañías aseguradoras (Perry, 2014) y farmacéuticas (La Minute Droit, 2014), una vez más, sin el consentimiento expreso del titular.

Por otra parte, un aspecto que revela la dificultad de control de los gigantes de internet es el tratamiento de grandes cantidades de información almacenadas por estas compañías. En la actualidad, el almacenamiento de datos se encuentra en expansión. Para dimensionar la cantidad de datos que existe en la *web*, solamente en Facebook se crean cada día diez terabytes, y en Twitter, siete terabytes (Demarthon *et al.,* 2013). Así, es posible que incluso los titulares desconozcan la existencia de un tratamiento de sus datos a causa del fenómeno del *Big data*.[15]

Gracias al *Big data* es posible asociar un volumen importante de datos en tiempo real. Más allá del simple almacenamiento de grandes cantidades de información, el *Big data* permite adquirir los datos y otorgarles un significado. Al respecto, las condiciones de licitud deben realizarse al momento de la recolección y no del tratamiento. Si el titular de los datos no es informado de las consecuencias del tratamiento del *Big data*, el tratamiento podría ser considerado como ilícito.

Finalmente, con el fin de dilucidar las problemáticas persistentes en materia de protección de datos a causa de la comercialización, a manera de ilustración, es posible citar el caso de Facebook:

1) Este gigante de internet tiene acceso a datos sensibles que gozan de especial protección, y conoce la tendencia política, orientación sexual de sus usuarios y puede, incluso, realizar reconocimiento facial. Esta compañía debería indicar cuál será la finalidad del tratamiento para cada dato personal recopilado, respetando la obligación de información y la naturaleza del dato, toda vez que la política de privacidad existente para el caso colombiano es general y ambigua.[16]

---

[15] El *Big data* es el crecimiento exponencial de los datos que supera la capacidad de almacenamiento de un software convencional. Con la existencia del *Big data* es posible, actualmente, por ejemplo, localizar en tiempo real a un titular de datos gracias a la geolocalización; predecir y prevenir enfermedades con el uso de los datos del paciente a partir de su anatomía, patologías, historia clínica, fisiología, entre otros.

[16] "¿Qué tipo de información recopilamos? Tus acciones y la información que proporcionas. Las acciones de otras personas y la información que proporcionan. Tus redes y conexiones. Información sobre pagos. Recopilamos información acerca de las computadoras, los teléfonos u otros dispositivos en los que instalas o desde los que accedes a nuestros servicios. Recopilamos información cuando visitas o usas sitios web y aplicaciones de terceros que usan nuestros servicios (por ejemplo, cuando ofrecen nuestro botón «Me gusta» o el inicio

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

2) Esta red social debería informar a sus usuarios sobre la transferencia de datos que efectúa a Estados Unidos. No obstante, la información no se encuentra disponible en la política de datos de Facebook.[17]
3) Facebook instala, igualmente, *cookies* espías, conocidas como *cookies DATR* en los computadores o aparatos móviles; estas *cookies* memorizan todas las visitas a páginas dotadas de un botón "me gusta" y recopilan la información de los internautas, incluso de aquellos que no son usuarios de la red. Todo lo anterior se realiza sin el consentimiento informado del usuario.[18]
4) Esta compañía conserva, asimismo, por un largo periodo la dirección IP del usuario que realiza la conexión en su red, sin su autorización (Leloup, 2011).

Por lo expuesto en estos cuatro puntos, es posible concluir que Facebook no respeta la legislación colombiana sobre protección de datos. Estas conductas han sido analizadas por la autoridad de protección de datos en Francia, quien ya ha solicitado a Facebook respetar la legislación en vigor (Untersinger, 2016). En Colombia, pese a que estas mismas infracciones se presentan, la autoridad encargada no ha iniciado ninguna investigación formal.

Una dificultad en el ejercicio del control consiste en que los gigantes de internet poseen varios mercados conexos interconectados entre sí, lo que facilita el tratamiento ilimitado de los datos. Así, una de las características principales de los gigantes de internet es la ausencia de determinación de una actividad principal. El objetivo de estas compañías consiste en tener

---

de sesión con Facebook, o cuando usan nuestros servicios de medición y publicidad). Dicha información incluye datos acerca de los sitios web y las aplicaciones que visitas, el uso que haces de nuestros servicios en dichos sitios web y aplicaciones, y los datos que el desarrollador o el editor de la aplicación o del sitio web te proporciona a ti o a nosotros" (Facebook, 2015b).

17 "La información recopilada dentro del Espacio Económico Europeo («EEE») puede, por ejemplo, transferirse a países que no pertenecen al EEE para asegurar el cumplimiento de los fines descritos en esta política" (Facebook, 2015a).

18 "Nuestros socios nos proporcionan información sobre ti y tus actividades tanto dentro como fuera de Facebook, por ejemplo, recibimos información de un socio cuando ofrecemos servicios de forma conjunta o datos de un anunciante acerca de tus experiencias o interacciones con éste... Las empresas pertenecientes a Facebook o administradas por Facebook nos proporcionan información sobre ti, de acuerdo con sus respectivas condiciones y políticas. Obtén más información sobre estas empresas y sus políticas de privacidad" (Facebook, 2015a).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

la mayor cantidad de clientes posibles, ofreciendo todos los servicios que requieren.

Estas compañías no realizan una distinción de servicios y de los diferentes tratamientos de datos ante las autoridades de control, así en apariencia pretendan cambiar su imagen. Google, por ejemplo, el año pasado creó su *holging Alphabetic* en agosto y cambió de nombre (Delsol, 2015); sin embargo, la ausencia de transparencia persiste. El Parlamento Europeo ya había propuesto en 2014 desmantelar Google con el fin de diferenciar sus actividades (Karayan, 2014), con la idea de realizar un control efectivo de cada una de las finalidades del tratamiento de datos que realizan.

Para finalizar, una problemática persistente es la explotación de los datos personales de las personas jurídicas localizadas en otro país; esto, en términos de competencia, genera el aumento de monopolios, casos de competencia desleal y abuso de posición dominante (sentencia Bottin Cartographes contra Google France, Google Inc., 2012).

Una vez examinadas las problemáticas originadas por la comercialización de datos, nos corresponde ahora presentar las proposiciones para asegurar la protección de los datos personales explotados por los gigantes de internet.

III. Los avances indispensables para asegurar la protección efectiva de los datos personales frente a la utilización por los gigantes de internet

Para asegurar la protección efectiva frente al uso de los datos personales por los gigantes de internet se presentarán a continuación dos grandes proposiciones generales para reforzar la protección existente:

1. *Proposiciones dentro del campo de aplicación material de la ley de datos personales y el ejercicio de control por parte de la autoridad competente*

Dentro de las proposiciones relacionadas en el campo de aplicación material, uno de los aspectos importantes es el establecimiento de la finalidad del tratamiento de datos, que en todos los casos deberá ser explícito y legítimo. Así, los datos no tendrían que ser tratados ulteriormente de forma incompatible con las finalidades establecidas inicialmente. La limitación de la finalidad del tratamiento es fundamental, en especial a nivel de las formalidades. La cuestión principal consiste en saber qué realizan con los datos estos gigantes de internet y no cuál es el objetivo del tratamiento.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

En consecuencia, las políticas de privacidad deben contener de forma explícita la finalidad, y en ningún caso ésta podría ser amplia o ambigua. A manera de ilustración, la política de privacidad que dice que los datos personales serán utilizados con finalidades de *marketing* no respeta la exigencia de determinación de la finalidad del tratamiento, toda vez que es imprecisa. En otras palabras, los gigantes de internet antes de realizar un tratamiento deberían definir concretamente: 1) qué datos se van a recolectar; 2) qué se va a efectuar como operación; 3) quién va a ser el responsable del tratamiento, y 4) cómo se va a organizar la información, quién va a tener acceso y si la información va a ser compartida. Toda esta información debería formar parte de la otorgada al momento de solicitar la autorización al titular de los datos.

Otro punto de vital importancia es el ejercicio del derecho de supresión. El responsable del tratamiento o el encargado debe proporcionar al titular de los datos, los mecanismos adecuados para presentar la solicitud de supresión. En la práctica se observa que estas herramientas no están al alcance de los titulares, quienes para poder suprimir un dato se pueden incluso ver condicionados a eliminar la cuenta, como en el caso de Facebook[19] o a incurrir en costos para formalizar la solicitud. Sobre este punto, la implementación de tecnologías que faciliten la eliminación efectiva de la información o el acceso ilimitado a la misma puede ser una solución. Herramientas como *Robots Exclusion Protocol* o *Vanish* permiten la autodestrucción de los datos por el solo paso del tiempo (Garriga, 2016: 241).

Ahora bien, en lo relacionado con los responsables del tratamiento y los encargados del tratamiento, se propone, de igual forma, reforzar sus obligaciones en caso de utilización secundaria de los datos del titular, piénsese, por ejemplo, en la implementación del *Big data*, por lo que se debería regular la conservación de los datos, limitando las posibilidades de reagrupar la información para identificar un titular y controlar el cruce de información (Zolynsky y Latreille, 2014: 275).

Otra proposición que surge a partir de la lectura de la Ley es la necesidad de consagrar una definición de destinatario de los datos personales. Esta definición es importante para verificar que la persona que efectúa el tratamiento de los datos se encuentra habilitado y bajo qué condiciones, toda vez que debe haber una restricción a un grupo limitado de personas con el fin de garantizar la intimidad del titular; esta restricción podría efec-

[19] "La información asociada a tu cuenta se conservará hasta que la cuenta se elimine, a menos que ya no necesitemos los datos para ofrecer los productos y servicios" (Facebook, 2015b).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

tuarse, igualmente, con la implementación de técnicas de cifrado para garantizar la confidencialidad y el acceso restringido al personal autorizado. El destinatario debería formar parte de la declaración que se tiene que presentar ante la autoridad encargada del control; así, por ejemplo, el responsable de recursos humanos de una empresa que recolecta datos no debería tener acceso a la información, o el servicio de *AdWords*[20] de Google no debería tener acceso a la información depositada por un titular en Google +.

Una definición que bien podría servir de ejemplo es la consagrada en el derecho francés, donde el destinatario es definido en esta legislación como "toda persona habilitada a recibir comunicación de sus datos" (artículo 3o., Ley 78-17 de 1978). Otra definición modelo se encuentra en el Reglamento europeo de 2016, que define al destinatario como una persona física o moral que recibe la comunicación de los datos personales, sea éste o no un tercero (artículos 4o. y 9o., Reglamento 2016/679).

En igual sentido, bien podríamos tomar como ejemplo los avances del nuevo Reglamento europeo sobre protección de datos personales (Reglamento 2016/679) para fortalecer por vía legislativa los derechos existentes de los titulares. Este Reglamento refuerza el derecho al olvido, y admite el derecho a la portabilidad de los datos al titular para facilitar su disposición. De igual forma, admite el derecho a ser informado sobre la piratería de sus datos (*Réforme sur la protection des données,* 2016) y reconoce el derecho a oponerse a la publicidad dirigida, que constituye una de las problemáticas más recurrentes en materia de protección de datos.

Es menester precisar que si bien la consagración legislativa contribuye al mejoramiento de la protección, los esfuerzos en Colombia deberán concentrarse en la actividad de control y sanción radicada en cabeza de la Superintendencia de Industria y Comercio. Por tal motivo, se abordarán a continuación las proposiciones sobre la efectividad del control por parte de la autoridad competente en materia de protección de datos personales.

Es indispensable que la autoridad encargada de la protección de datos personales sea independiente de las otras entidades del sector público, esto con el fin de asegurar la neutralidad e imparcialidad y de evitar los conflictos de interés en la toma de decisiones, toda vez que el responsable o el encargado del tratamiento puede ser una persona de naturaleza pública. La Commission Nationale de l'informatique et des Libertés "CNIL" (Ley 78-17 de 1978) es un modelo de entidad encargada de la protección de datos personales, cuya organización garantiza su independencia. Los elementos que caracterizan su imparcialidad son: 1) la existencia de un cuerpo colegiado,

[20] Es el servicio de venta de publicidad dirigida de Google.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

en su caso, de diecisiete miembros, integrado por magistrados, senadores, diputados y personas especializadas en el tema de protección de datos personales; 2) la irrevocabilidad de sus miembros, salvo los casos de renuncia, y 3) la incompatibilidad de ejercer funciones políticas o cargos dentro de una persona jurídica.

En igual sentido, garantizar la independencia de esta autoridad es indispensable para poder efectuar un control sobre el tratamiento de datos realizado por las autoridades públicas colombianas. Las instituciones públicas tienen la facultad de acceder a los datos personales de los individuos;[21] un reto para la autoridad encargada de la protección de datos consistirá en encuadrar estos tratamientos de datos personales.

De otra parte, sobre el ejercicio del control realizado por el Departamento para la protección de datos personales, a manera de proposición, éste debería ejecutarse de forma previa y posterior a la realización del tratamiento de datos. Asimismo, la implementación de un sistema de auditoría sería de gran utilidad, toda vez que sólo la autorización no controla la puesta en marcha del tratamiento.

Ahora bien, sobre las proposiciones relacionadas con las sanciones, éste es, sin lugar a dudas, uno de los temas más críticos de la Ley colombiana de protección de datos de 2012, toda vez que, como ya se indicó (véase *supra*: 8), los montos de las sanciones pecuniarias impuestas no generan ningún efecto disuasivo para los gigantes de internet, de manera que el refuerzo de las sanciones debería tener lugar, igualmente, en Colombia. Un ejemplo de los avances en materia de sanciones se presentó recientemente para las autoridades de protección de datos en Europa con la adopción del nuevo Reglamento sobre protección de datos personales (Reglamento 2016/679). A partir de la entrada en vigor del Reglamento (25 de mayo de 2018), las sanciones administrativas podrán afectar hasta el 4% del volumen de ventas mundial de las compañías de internet (CNIL, 2016).

Para finalizar, es necesario incrementar la conciencia de los titulares sobre el valor de la información que dejan a su paso en la *web*, conciencia que aún no existe en Colombia. La tarea de sensibilización debería formar parte de las funciones de la autoridad encargada de la protección de datos. Ninguna legislación sobre la protección de datos personales será suficiente si internet no encuentra su base en la confianza.

[21] El control del tratamiento de datos por entidades públicas es indispensable. Ejemplo, en la actualidad, la National Security Agency (NSA) construyó el más grande centro de interceptaciones de comunicación (NSA, 2010), con capacidad para almacenar *yottaoctets* de información recolectada en internet (Bernard, 2013).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

2. *Proposiciones sobre el ámbito territorial frente al uso de los datos personales por los gigantes de internet*

La transferencia de datos personales hacia países que carecen de un régimen de protección de datos personales o que no proporcionan un nivel adecuado de protección es un tema que debe ser objeto de atención. En Colombia, el "principio" es la prohibición de transferencia de datos hacia países que no brindan un nivel adecuado de protección. Es importante aclarar que un "nivel adecuado" no obliga al país donde se va a realizar el tratamiento a asegurar de manera idéntica la protección. Es suficiente con que el nivel sea sustancialmente equivalente (Perray y Uzan-Naulin, 2015: 2), precisando que esta apreciación será competencia de la autoridad colombiana de protección de datos y no del responsable del tratamiento (Perray, 2014: 218).

Ahora bien, la Ley colombiana contempla un "régimen de excepción" en una lista taxativa para transferencia de datos (artículo 26, Ley Estatutaria Núm. 1581 de 2012). En los casos no contemplados como excepción, la Superintendencia de Industria y Comercio deberá ser quien otorgue la declaración de conformidad para estas transferencias internacionales de datos. No obstante, en la práctica el control sobre las transferencias internacionales de datos no es suficiente, por lo cual una actuación al respecto se hace indispensable (Remolina, 2015).

Por otro lado, a pesar de la reglamentación vigente en Colombia, aún no forma parte de los países considerados con un nivel adecuado de protección de datos personales; esto se debe probablemente a que la reglamentación es reciente y no ha habido una promoción a nivel mundial sobre estos avances. En el caso de Europa, la Comisión Europea ha reconocido únicamente a doce países un nivel adecuado de protección,[22] de los cuales en América Latina sólo Argentina y Uruguay forman parte[23] (CPVP, s.a. b).

Estados Unidos, gran potencia en prestación de servicios de internet y país en el cual residen los gigantes de internet, no cuenta con niveles de protección equiparables a los del derecho colombiano. Esto obedece a que el régimen jurídico americano aplica la acepción "patrimonialista", que considera los datos personales como bienes susceptibles de ser enaje-

[22] La Comisión Europea reconoce parcialmente un nivel adecuado de protección para Canadá, por los tratamientos sometidos a la ley canadiense "Personal Information Protection and Electronic Documentation Act" y para los datos relativos a los pasajeros aéreos. Australia también se considera con niveles adecuados de protección para este tipo de datos.

[23] Los otros países son Suiza, Andorra, Guernesey, Isla de Man, las Islas Feroe, Jersey, Israel y Nueva Zelanda.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

nados, promoviendo de esta manera el crecimiento económico, mientras que en el modelo colombiano se aplica la acepción "personalista", que considera a los datos personales como un atributo de la personalidad, de manera que en principio la transferencia de datos hacia Estados Unidos debería ser prohibida. Esta discrepancia entre regímenes dificulta la protección de los datos personales, de ahí que la conciliación entre los dos regímenes sea necesaria.

El modelo americano ha avanzado en este sentido; recientemente surgió una iniciativa: el proyecto de Ley Federal Data Brokers Accountability and Transparency Act (DATA, 2015), que plantea la introducción de reglas como el derecho a la información, el derecho de acceso y oposición. De esta manera, el derecho americano ha comenzado a acercarse a la concepción personalista de tendencia europea (Castets-Renard, 2016b: 115) y, en consecuencia, a la concepción colombiana.

Existe una influencia recíproca de sistemas jurídicos disímiles (el modelo europeo no es ajeno a este fenómeno) y la adopción del nuevo Reglamento de datos personales es un claro ejemplo, ya que los responsables del tratamiento después de la entrada en vigor en 2018 no estarán sometidos a un control formal a priori por las autoridades, sino a un control a posteriori, que se traduce en la obligación de rendir cuentas o *accountability* (Castets-Renard, 2016b: 115).

Con el fin de resolver las diferencias de regímenes, en el caso europeo, hasta el 2015, el destinatario de los datos en Estados Unidos podía adherirse a "los principios de la esfera de seguridad" o *Safe Harbor Principles*[24] para efectuar la transferencia de datos.[25] Este acuerdo fue invalidado por la CJUE (Sentencia del caso C-362/14, 2015), al considerar que Estados

[24] Los principios de *Safe Harbor* —o esfera de seguridad— fueron creados en conjunto entre el Departamento de Comercio americano y la Comisión Europea. Estos principios tenían por objetivo primordial facilitar y garantizar la transferencia de datos personales de Europa a Estados Unidos. Las sociedades americanas que se adherían a estos principios se encontraban sometidas al control de la Federal Trade Commission, que para el caso del *Safe Harbor* era la autoridad americana encargada de examinar si las empresas respetaban las obligaciones previstas; gracias a la implementación *del Safe Harbor* se entendía que estas empresas ofrecían un nivel adecuado de protección de acuerdo con la reglamentación europea (CPVP, s.a. a).

[25] Los gigantes de internet continúan prevaliéndose del acuerdo *Safe Harbor*. Por ejemplo, dentro de la política de privacidad de Facebook se indica que "Facebook, Inc. cumple con el marco *Safe Harbor* de los Estados Unidos y la Unión Europea y de los Estados Unidos y Suiza para la recopilación, el uso y la retención de datos pertenecientes a la Unión Europea y a Suiza, según lo dispuesto por el Departamento de Comercio de los Estados Unidos. Para ver nuestra certificación, visita el sitio web del programa *Safe Harbor*" (Facebook, 2015b).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

Unidos no protege de forma suficiente los datos de los titulares europeos[26] (Naftalski, 2016: 340). La decisión fue, igualmente, motivada por razones económicas ligadas a la protección del mercado interno europeo y por las revelaciones de Edward Snowden de 2013 (Castets-Renard, 2016a: 88).

Las consecuencias económicas de esta decisión fueron previsibles, toda vez que "el número de empresas americanas adherentes a *Safe Harbor* era de 3,300 y el 51% de las empresas certificadas realizaban tratamientos de datos de asalariados residentes en Europa. La perturbación del flujo de datos trasatlántico hubiera podido tener un impacto recesivo sobre el PIB de la Unión estimado entre -0,8% y -1,3%" (Perray, 2015: 2). Motivo por el cual un segundo acuerdo entre la Unión Europea y Estados Unidos no se hizo esperar. Actualmente, la transferencia deberá tener en cuenta el acuerdo de *Privacy Shield*, concluido entre la Unión Europea y Estados Unidos, cuyo objetivo es proteger, por una parte, los derechos fundamentales de los ciudadanos europeos, y por otra, otorgar seguridad jurídica a los responsables del tratamiento de los datos[27] (Merav, 2016: 1).

A pesar de las garantías, el acuerdo de *Privacy Shield* ha sido criticado en Europa, especialmente porque los procedimientos de solicitud de protección son complejos para el titular de los datos y porque hace alusión a la Directiva de 1995 —que dentro de dos años será derogada por el Reglamento de 2016—. La CNIL ha expresado recientemente su preocupación, toda vez que el texto no especifica la exclusión de los tratamientos masivos e indeterminados de los datos personales que provienen de Europa.[28] Aunque es muy prematuro juzgar la eficacia de dicho acuerdo, con lo anteriormente citado se puede evidenciar que las dificultades existentes en Colombia persisten también en la Unión Europea, donde el problema de la protección internacional de los datos aún no ha sido resuelto.

En Colombia, por su parte, no existe ningún acuerdo de transferencia de datos personales con Estados Unidos; la dificultad en nuestro caso reside en el poder de negociación del Estado colombiano. La Corte Cons-

[26] La decisión fue fundamentada con base en los artículos 7o. y 8o. de la Carta de los Derechos Fundamentales de la Unión Europea: el primero consagra el derecho a la vida privada que tiene toda persona, y el segundo, a la protección de los datos personales.

[27] Este acuerdo refuerza las garantías del antiguo acuerdo *Safe Harbor*, imponiendo obligaciones adicionales a las empresas americanas, limitando los poderes de vigilancia de las autoridades públicas americanas y reforzando el control ejercido por el ministro de comercio y la Federal Trade Commission (FTC); de igual forma, el acuerdo *Privacy Shield* obliga a Estados Unidos a cooperar con las autoridades europeas (Merav, 2016: 1).

[28] Las autoridades encargadas de la protección de datos en Europa se preocupan en especial porque el texto no contiene detalles acerca de las recopilaciones masivas e indeterminadas de datos personales provenientes de Europa (Pépin, 2016).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

titucional considera que los niveles apropiados de protección son satisfechos si la legislación del país cuenta "con unos principios que abarquen obligaciones y derechos de las partes y de los datos; y con un procedimiento de protección que involucre mecanismos y autoridades que efectivicen la protección de la información" (Sentencia C-748/11). Estas exigencias deberán tenerse en cuenta en una eventual negociación.

Ahora bien, tratándose de transferencias de datos personales de Colombia hacia otros países realizadas por un grupo empresarial o una multinacional, las Binding Corporate Rules (BCR) o Normas Corporativas Vinculantes (NCV)[29] facilitan la transferencia internacional de datos. Ese reglamento interior va a determinar la política de confidencialidad de una multinacional, cualquiera que sea la implantación en el mundo de sus filiales.[30] A manera de proposición sobre las NCV, es recomendable, asimismo, implementar procedimientos de auditoría interna para asegurar el respeto de la legislación por las NCV (Perray, 2015: 2). Tratándose de sectores económicos específicos, como el farmacéutico o el financiero, la adopción de códigos de conducta[31] que obliguen al responsable del tratamiento podría ser la solución apropiada en razón de los contenidos particulares de los datos tratados (Naftalski, 2016: 340).

En lo concerniente a las sanciones, a nivel latinoamericano se debería reforzar la colaboración entre Estados. A pesar de no encontrarnos en el mismo nivel de integración legislativa, la colaboración existente entre las autoridades europeas es un modelo a seguir. El nuevo Reglamento de protección de datos europeo permite emitir sanciones conjuntas o con colaboración entre autoridades de los países miembros de la Unión.

---

29 Las Binding Corporate Rules (BCR) son principios de buen gobierno o reglas de buenas prácticas que son creadas por las organizaciones y que cuentan con fuerza vinculante para sus miembros, las cuales se constituyen como códigos internacionales de conducta y tienen por objetivo proteger el flujo de los datos personales. Las BCR permiten realizar las transferencias de datos personales, siempre que las entidades de un mismo grupo empresarial aseguren que cuentan con niveles equiparables a los contenidos en la ley colombiana de 2012, aun si la entidad situada en el exterior está establecida en un país que no cuenta con los niveles adecuados de protección.

30 En todos los casos, las NCV deberán contener la autorización expresa del titular, la aprobación de las NCV por la autoridad pública encargada de la protección de datos. Esta autoridad deberá brindar asistencia a los titulares de la información para el ejercicio y control de sus derechos, y establecer mecanismos para presentar recursos cuando los derechos se vean vulnerados o se evidencien perjuicios por el no respeto de las normas.

31 Los códigos de conducta surgen a partir del compromiso del responsable del tratamiento o del encargado (ubicados fuera del país); estos códigos tienen por vocación ofrecer las garantías apropiadas, comprendiendo, entre otras cosas, los derechos de los titulares de la información.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

La extraterritorialidad del tratamiento de datos personales exige la adopción de medidas de colaboración entre las entidades encargadas de ejercer el control. La cooperación internacional actual resulta insuficiente, toda vez que sólo el 36% de países en el mundo cuentan con una autoridad encargada (Remolina, 2015). En el modelo europeo, un organismo supranacional ha sido creado: el Comité Europeo de Protección de Datos,[32] que será el organismo de última instancia encargada de dirimir los conflictos entre las autoridades de cada país miembro; igualmente, este Comité será competente para emitir conceptos con fuerza obligatoria y elaborar la doctrina europea en la materia. En América Latina, la cooperación entre Estados podría contribuir a garantizar la protección de los datos.

IV. Conclusiones

Es importante defender la idea de la protección de los datos personales como un atributo de la personalidad, proteger la intimidad de los individuos y luchar contra los paraísos de datos personales que se encuentran en varios países del mundo. A pesar que la protección de datos es permeable frente al avance de las tecnologías de la información, la transparencia de los terceros países y al uso de los datos por los grandes actores de internet que tienen el monopolio, Colombia hoy en día ha avanzado en la positivización de niveles adecuados de protección.

Las políticas de privacidad de los gigantes de internet no protegen los datos personales. Es necesario fortalecer las herramientas con las cuales ya contamos, a fin de ejercer un control activo sobre el tratamiento de los datos. El fenómeno de la internacionalización de los datos constituye un desafío fundamental para la protección, así como la posibilidad de ejercer el derecho a la supresión de datos. Pese a los avances logrados en Colombia en materia de regulación de datos personales, varios retos persisten.

El control efectivo de la transferencia internacional de datos personales hacia países que no cuentan con un nivel adecuado de protección, toda vez que sólo el 22% de la población mundial vive en países con normas generales de protección (Remolina, 2015: 133) y el volumen de intercambio de datos con los países que garantizan la protección de datos es marginal con respecto a los flujos internacionales (Perray, 2014: 221).

El segundo reto consiste en preservar la vida privada de los titulares, asegurando un consentimiento libre, expreso e informado para cada una de las finalidades del tratamiento de datos personales. Otro de los retos pre-

[32] Este organismo sustituye al hoy existente Comité del artículo 29.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

sentes es asegurar la libre competencia del mercado interno, examinando la regulación como un instrumento de desarrollo económico.

La utilización de los datos personales por los gigantes de internet vulnera las disposiciones colombianas vigentes sobre protección de datos personales, y en su estado actual es posible evidenciar que el tratamiento de datos personales no cumple con las exigencias contenidas en la ley. La aplicación de sanciones es indispensable en este punto, y el papel de la autoridad encargada de proteger los datos personales es preponderante, pues ella deberá ser quien garantice su independencia. La propuesta del incremento pecuniario de las sanciones podría generar un efecto disuasivo en la comercialización abusiva de los datos personales. Es indispensable afianzar las labores de la autoridad competente para asegurar su independencia e imparcialidad.

V. Fuentes de información

Bernard, Philippe, 2013, "Au cœur de l'Utah, les États-Unis déploient leurs «grandes oreilles»", *Le Monde*, París, 12 de junio, disponible en: *http://www.lemonde.fr/ameriques/article/2013/06/12/au-c-ur-de-l-utah-les-etats-unis-deploient-leurs-grandes-oreilles_3428568_3222.html* (fecha de consulta: 18 de febrero de 2016).

Castets-Renard, Céline, 2016, "Invalidation du Safe Harbor par la CJUE: tempête sur la protection des données personnelles aux États-Unis", *Recueil Dalloz*, París, núm. 2, 14 de enero.

———, 2016, "Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles?", *Dalloz IP/IT*, París, núm. 3, 10 de marzo.

Commission de la Protection de la Vie Privée (CPVP), s.a. a, *Safe Harbor Principles (ou Principes de la sphère de Sécurité) CPVP*, Bélgica, Privacy Commission, disponible en: *http://www.privacycommission.be/fr/lexique/safe-harbor-principles* (fecha de consulta: 2 de marzo de 2016).

———, s.a. b, *Transferts en dehors de l'UE-niveau de protection adéquat CPVP,* Bélgica, Privacy Commission, disponible en: *http://www.privacycommission.be/fr/en-dehors-ue-protection-adequate* (fecha de consulta: 2 de marzo de 2016).

Conseil National Informatique et Libertes (CNIL), 2016, *Adoption du règlement européen par le Parlement européen: un grand pas pour la protection des données en Europe,* París, 14 de abril, disponible en: *https://www.cnil.fr/fr/adoption-du-reglement-europeenparleparlementeuropeen-un-*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

grand-pas-pour-la-protection-des-donnees (fecha de consulta: 18 de abril de 2016).

———, s.a., *Les cookies,* París, disponible en: *http://www.cnil.fr/vos-droits/vos-traces/les-cookies/* (fecha de consulta: 10 de abril de 2016).

Constitución Política de Colombia, 1991, Colombia, Asamblea Nacional Constituyente.

Decreto 1377 de 2013, Colombia, Presidencia de la República de Colombia, 27 de junio de 2013.

Delsol, Emmanuelle, 2015, *Alphabet ou l'illusion de la transparence, l'usine digitale*, París, L'usine digitale, 19 de agosto, disponible en: *http://www.usinedigitale.fr/editorial/alphabetoulillusiondelatransparence.N345289* (fecha de consulta: 2 de febrero de 2016).

Demarthon, Fabrice *et al*., 2013, *CNRS International Magazine, The Big Data Revolution*, París, núm. 28, enero, disponible en: *http://www.cnrs.fr/fr/pdf/cim/28/#/1/* (fecha de consulta: 28 de abril de 2016).

Directiva 95/46/CE, Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 1995, Parlamento Europeo y del Consejo, *Diario Oficial* Núm. L 281, de 23 de noviembre de 1995.

Escande, Philippe, 2016, "Google, Apple et le prix du rêve", *Le Monde Économie*, París, 2 de febrero, disponible en: *http://www.lemonde.fr/economie/article/2016/02/02/googleappleetleprixdureve_4857945_3234.html* (fecha de consulta: 20 de mayo de 2016).

Facebook, 2015a, *Full Data Use Policy of Facebook*, Estados Unidos, 30 de enero, disponible en: *https://es-la.facebook.com/full_data_use_policy* (fecha de consulta: 30 de mayo de 2016).

———, 2015b, *Privacy Explanation of Facebook*, Estados Unidos, 30 de enero, disponible en: *https://es-la.facebook.com/privacy/explanation* (fecha de consulta: 29 de mayo de 2016).

Garriga, Ana, 2016, *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*, Madrid, Dykinson.

Jaimes, Nicolas, 2015, "Le chiffre d'affaires de Google en hausse de 12% au premier trimestre", *Journal Du Net JDN*, París, disponible en: *http://www.journaldunet.com/ebusiness/lenet/googlechiffredaffaires1ertrimestr-2015-0415.shtml* (fecha de consulta: 13 de abril de 2016).

Karayan, Raphaële, 2014, "Google est-il vraiment menacé de démantèlement en Europe?", *L'express*, París, 27 de noviembre, disponible en: *http://lexpansion.lexpress.fr/hightech/googleestilvraimentmenacededemantelement-en-europe_1626395.html* (fecha de consulta: 3 de marzo de 2016).

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

La Minute Droit, 2014, *Base de données et droit de la concurrence*, Francia, 19 de agosto, disponible en: *http://laminutedroit.com/base-donnees-droit-concurrence/* (fecha de consulta: 13 de abril de 2016).

La Redacción de Diario Le Monde, 2012, "Facebook franchit la barre du milliard d'utilisateurs", *Le Monde,* París, 4 de octubre, disponible en: *http://www.lemonde.fr/technologies/article/2012/10/04/facebookfranchitla barre-du-milliard-d-utilisateurs_1770255_651865.html* (fecha de consulta: 13 de abril de 2016).

La Redacción de Journal Du Net Jdn, 2016, *Parts de marché des moteurs de recherche dans le monde*, París, 6 de enero, disponible en: *http://www.journaldunet.com/ebusiness/lenet/1087491partsdemarchedesmoteurs-de-recherche-dans-le-monde/* (fecha de consulta: 18 de marzo de 2016).

La Redacción de La Tribune, 2014, "Droit à l'oubli, Google condamné au Japon, Taubira veut protéger la presse", *La Tribune*, Francia, 10 de octubre, disponible en: *http://www.latribune.fr/technosmedias/internet/20141010trib19fafb27f/droitbgoola* (fecha de consulta: 15 de abril de 2016).

Leloup, Damien, 2011, "Facebook accusé de conserver des données effacées et de créer des profils fantômes", *Le Monde*, París, 24 de octubre, disponible en: *http://www.lemonde.fr/technologies/article/2011/10/24/facebookaccusedeconservedesdonneeseffaceesetdecreerdesprofilsfantomes_1592814_651865.html* (fecha de consulta: 31 de mayo de 2016).

Ley 25.326. Ley de protección de datos personales, Argentina, Senado-Cámara de Diputados de la Nación de Argentina, 2000.

Ley 78-17. *Relative à l'informatique, aux fichiers et aux libertés*, Francia, Asamblea Nacional y Senado de Francia, 6 de enero de 1978.

Ley Estatutaria Núm. 1266 de 2008. Por la cual se dictan las disposiciones generales del *Habeas Data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, Colombia, Congreso de la República de Colombia, 31 de diciembre de 2008.

Ley Estatutaria Núm. 1581 de 2012. Por la cual se dictan las disposiciones generales para la protección de datos personales, Colombia, Congreso de la República de Colombia, 17 de octubre de 2012.

Merav, Griguer, 2016, *Le Safe Harbor est mort, vive l'UE-US Privacy Shield Arrangement*, París, Lexisnexis, Cahiers de droit de l'entreprise, núm. 2.

Naftalski, Fabrice, 2016, "L'impact du nouveau règlement sur les stratégies de transferts internationaux des données personnelles", *Dalloz IP/IT*, París, núm. 7, 12 de julio.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

National Security Agency (NSA), 2010, *NSA Awards a Multi-Year IDIQ Umbrella Contract and the 1st Technical Task Order (TTO) to the Military Installation Development Authority for Supplying the Utilities Infrastructure to the Camp Williams, Utah Data Center Project Site, Utah data center,* Estados Unidos, 28 de mayo, disponible en: *https://www.nsa.gov/news-features/press-room/press-releases/2010/idiq-contract.shtml* (fecha de consulta: 22 de mayo de 2016).

Neilime, Emilien, 2015, *iPhone, Apple grappille des parts de marché à Samsung,* 24 de julio, disponible en: *http://www.macplus.net/depeche-84479-iphone-apple-grappille-des-parts-de-marche-a-samsung* (fecha de consulta: 7 de marzo de 2016).

Pépin, Guénaël, 2016, *Le Parlement européen adopte le règlement sur les données personnelles et le PNR*, París, Nextinpact, 14 de abril, disponible en: *http://www.nextinpact.com/news/99480-le-parlement-europeen-adopte-reglement-sur-donnees-personnelles-et-pnr.htm* (fecha de consulta: 20 de abril de 2016).

Perray, Romain, 2014, en Martial-Braz, Nathalie (dir.), *La proposition de règlement européen relatif aux données à caractère personnel: propositions du réseau Trans Europe experts*, París, Société de Legislation Comparée, colección Trans Europe Experts.

——— y Uzan-Naulin, Julie, 2015, "Arrêt Schrems: Cour(s) magistral(e) de droit à la protection des données personnelles", *LexisNexis*, París, étude 21, Communication Commerce électronique núm. 12.

Perry, Charles, 2014, *Apple Iwatch: vos données médicales vendues aux compagnies d'assurance?*, Francia, Objet connecté, 25 de agosto, disponible en: *http://www.objet-connecté.eu/mobilite/apple-iwatch-vos-donnees-medicales-vendues-aux-compagnies-dassurance-112192014.html* (fecha de consulta: 13 de abril de 2016).

Prodhan et Harro Ten Wolde, Georgina, 2016, "Facebook soupçonné d'abus de position dominante en Allemagne", *Reuters*, Londres-París, 2 de marzo, disponible en: *http://fr.reuters.com/article/technologyNews/idFRKCN0W410F?pageNumberandChannel=0* (fecha de consulta: 5 de abril de 2016).

Proyecto de Ley Federal Data Brokers Accountability and Transparency Act (DATA), 2015, Estados Unidos, Senado, disponible en: *http://www.markey.senate.gov/imo/media/doc/20150304DataBrokersBillText2f* (fecha de consulta: 2 de mayo de 2016).

Rauline, Nicolas, 2015, *Nouvelle charge des auteurs contre Amazon aux Etats-Unis*, Francia, Les Echos, 21 de agosto, disponible en: *http://www.*

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

lesechos.fr/21/08/2015/lesechos.fr/021274776921_nouvellechargm (fecha de consulta: 12 de enero de 2016).

"Réforme sur la protection des données", *La Semaine Juridique Entreprise et Affaires*, París, núms. 16-17, act. 356, 21 de abril de 2016.

Reglamento 2016/679. Reglamento general sobre la protección de datos RGPD, relativo a la protección de personas naturales frente al tratamiento de los datos personales y la libre circulación de sus datos, que abroga la directiva 95/46/CE, 27 de abril de 2016, Parlamento Europeo y del Consejo.

Remolina, Nelson, 2015, *Recolección internacional de datos personales: un reto del mundo post-internet,* Madrid, Agencia Española de Protección de Datos.

Resolución Núm. 4046. Por la cual se resuelve una solicitud de bloqueo temporal de datos, Colombia, Superintendencia de Industria y Comercio de Colombia, 2015.

Rochfeld, Judith, 2015, *L'effectivité du droit face à la puissance des géants de l'Internet*, en Behar-Touchais, Martine (dir.), París, Institut de Recherche Juridique de la Sorbonne IRJS éditions.

Sentencia Bottin Cartographes *vs.* Google France, Google Inc., Tribunal de Commerce de Paris TCP, París, 31 de enero de 2012.

Sentencia C-748/11, Corte Constitucional de Colombia, magistrado ponente: Jorge Ignacio Pretelt Chaljub, Colombia, 6 de octubre de 2011.

Sentencia del caso C-131/12, Agencia Española de Protección de Datos (AEPD) y Mario Costeja González *vs*. Google Spain, S. L. y Google Inc., 13 de mayo de 2014, Tribunal de Justicia de la Unión Europea, Gran Sala, Unión Europea, disponible en: *http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d5595b65b3a742c9b944bda7953befc2.e34KaxiLc3qMb40Rch0SaxuNbh90?tex=&dcid=152065&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=&cid=1212* (fecha de consulta: 29 de abril de 2016).

Sentencia del caso C362/14, Maximillian Schrems *vs.* Data Protection Commissioner, 6 de octubre de 2015, Tribunal de Justicia de la Unión Europea, Gran Sala, Unión Europea, disponible en: *http://curia.europa.eu/juris/document/document.jsf?docid=169195* (fecha de consulta: 3 de marzo de 2016).

Sentencia Google France, Google Inc./Bottin Cartographes, París, Cour d'appel de Paris Pôle 5-chambre 4, 20 de noviembre de 2013.

Sentencia T-462/97, 24 de septiembre de 1997, autoridad responsable: Corte Constitucional, magistrado ponente: Vladimiro Naranjo Mesa, Colombia.

DOI: http://dx.doi.org/10.22201/iij.25940082e.2017.3.10823

SLICE42 GROUP, 2015, "iPhone, Apple grappille des parts de marché à Samsung", Dijon, 24 de julio, disponible en: *http://www.macplus.net/depeche84479iphoneapplegrappilledespartsdemarche-a-samsung* (fecha de consulta: 15 de marzo de 2016).

TIROLE, Jean, 1993, *Théorie de l'organisation industrielle*, Francia, Económica (2015, nueva reimpresión en un único volumen).

UNTERSINGER, Martin, 2016, "Données personnelles: le virulent réquisitoire de la CNIL contre Facebook", *Le Monde*, París, 9 de febrero, disponible en: *http://www.lemonde.fr/pixels/article/2016/02/09/donneespersonnellesle virulentequisitoiredelacnilcontrefacebook_4861621_4408996.html* (fecha de consulta: 15 de marzo de 2016).

ZOLYNSKI, Célia y LATREILLE, Antoine, 2014, "Nouvelles pratiques: faut-il de nouvelles protections?", *La proposition de règlement européen relatif aux données à caractère personnel proposition du réseau Tran Europe Experts*, París, Société de Législation Comparée, vol. 9.