Fecha de recepción: 31 de agosto de 2016 / Fecha de aprobación: 28 de noviembre de 2016

Revista de Derecho Comunicaciones y Nuevas Tecnologías

BIG DATA: HACIA LA PROTECCIÓN DE DATOS PERSONALES BASADA EN UNA TRANSPARENCIA Y RESPONSABILIDAD AUMENTADAS

MIGUEL RECIO GAYO

Artículo de reflexión

DOI: http://dx.doi.org/10.15425/redecom.17.2017.09

Universidad de los Andes
Facultad de Derecho
Rev. derecho comun. nuevas tecnol. No. 17
enero - junio de 2017. e-ISSN 1909-7786

Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas

Resumen

Todo está cambiando rápidamente y esto supone que debamos considerar específicamente algunos conceptos como el de privacidad, al igual los principios que hasta el momento se venían aplicando, por ejemplo, los relativos a la información y al consentimiento. Aplicados al tratamiento de datos personales, estos principios ya no son eficientes si pensamos en la realidad actual y en el futuro. El uso de los resultados de un tratamiento analítico de datos personales masivos es, por lo tanto, a lo que hay que prestar atención a la hora de proteger a la persona, para evitar que los beneficios que puede aportar dicho tratamiento se vean empañados por consecuencias negativas, como la discriminación. La transparencia y la responsabilidad aumentadas serán los principios fundacionales de la protección de datos personales y la privacidad, siendo además una oportunidad de promover normas robustas, claras y adaptables, incluso a nivel global.

Palabras clave: datos personales, privacidad, derecho a la protección de datos, *big data*, consentimiento, información, transparencia, responsabilidad.

Big data: towards the protection of personal data based on an improved transparency and accountability

Abstract

Everything is rapidly changing and this means that we need to consider specifically certain concepts, such as privacy, and the principles that so far had been applied, as for example, the information and consent principles. With regard to the processing of personal data, those principles are no longer efficient if we think in the current reality and in the future. The use of the results of personal big data analytics is, therefore, to which we must pay attention to protect the person, so the benefits that such processing can bring do not be obscured by negative consequences, such as discrimination. Improved transparency and accountability will be the founding principles of the protection of personal data and privacy, being furthermore an opportunity to promote robust, clear, and flexible standards even globally.

Keywords: personal data, privacy, right to data protection, big data, consent, information, transparency, accountability.

Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas*

MIGUEL RECIO GAYO**

SUMARIO

* Cómo citar este artículo: Recio Gayo, M. (Junio, 2017). *Big data*: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* (17). Universidad de los Andes (Colombia). http://dx.doi.org/10.15425/redecom.17.2017.09

** Doctorando. Máster en Derecho de la Propiedad Intelectual por The George Washington University Law School y Máster en Protección de Datos, Transparencia y Acceso a la Información por la Universidad San Pablo-CEU. Licenciado en Derecho por la Universidad Carlos III de Madrid. Correo: miguelrecio@miguelrecio.com

Introducción

El fenómeno *big data*, término que puede traducirse al español como datos masivos, es una cuestión trascendental tanto para la economía digital como para la sociedad. A los datos masivos, cuando son datos personales, se han referido ya muchos expertos y autoridades, pudiendo resaltar que en el dictamen preliminar titulado *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, el Supervisor Europeo de Protección de Datos (SEPD) los consideró el "petróleo de la economía digital" (2014, p. 8).

Vistos como una revolución, los datos masivos y la analítica computacional (*analytics*) están en plena expansión ascendente y no tienen fronteras. Tal y como ha señalado la Comisión Europea "se espera que la tecnología y los servicios de los macrodatos representen un valor mundial de 16 900 millones USD" (2014, p. 2).

Los datos personales masivos y su tratamiento analítico pueden conllevar importantes beneficios, que se concretan tanto en oportunidades de innovación en el caso de servicios electrónicos, por ejemplo las aplicaciones para dispositivos móviles o apps, como de nuevas formas de tratar enfermedades, incluso reduciendo los costos de tratamientos que hoy no son accesibles para todas las personas. Al respecto, la International Conference of Data Protection and Privacy Commissioners (ICDPPC) en su Resolución sobre *big data* ha indicado:

> Se afirma con frecuencia que la capacidad de almacenar y analizar grandes cantidades de datos puede ser benéfica para la sociedad. El *big data* (metadatos) puede utilizarse, por ejemplo, para predecir la propagación de epidemias, descubrir los graves efectos secundarios de medicamentos y combatir la contaminación en las grandes ciudades. (2014, p. 1).

Esto, que actualmente sigue siendo visto como una revolución, la de los datos masivos, implica ya e implicará cambios en muchos sentidos y, sobre todo, supone que desde hace ya algunos años se haya iniciado un profundo análisis, al menos por parte de algunos países, que debería dar lugar a un debate internacional para buscar, preferiblemente, una aproximación global que sirva para establecer un marco adecuado para la innovación, la privacidad y la protección de los datos personales.

Cuando el análisis de los datos masivos (*big data analytics*) incluye datos personales, resulta necesario examinar desde el punto de vista del cambio regulatorio y de paradigma las implicaciones que pueda tener para sus titulares pasar de "la «privacidad por consentimiento» a la «privacidad a través de la responsabilidad»" como indican, entre otros, Mayer-Schönberger y Cukier (2013, p. 215), a la que puede y debe añadirse la transparencia.

Además, el tratamiento de los datos masivos implica la necesidad de considerar las rela-

ciones que pueden darse entre quien recaba, obtiene o recolecta los datos personales (*data collector*), ya sea una entidad pública o una empresa u organización del sector privado; quien los trata (*data analyzer*) y quien los usa (*user of the analyzed data*). En el caso de la persona física a la que se refieren los datos, ya no es una mera cuestión de consentimiento, legitimación o licenciamiento para el uso o explotación de los datos recolectados y analizados, sino de garantizar la responsabilidad (*accountability*) a lo largo de toda la cadena de tratamiento de los datos masivos y hacerlo de manera transparente, cuando se trate de sus datos personales.

Y serán estas cuestiones, prestando especial atención a las implicaciones que el *big data* pueda tener para la protección de datos personales y la privacidad, las que se pretende atender a continuación, teniendo en cuenta que pueden ser relevantes para el futuro marco aplicable a la protección de los datos personales y la privacidad. En concreto, las políticas públicas sobre protección de datos y privacidad, por las implicaciones que pueden tener los datos masivos y su tratamiento analítico, requieren comprender el pasado para, en la medida de lo posible, aplicarlo en los próximos años; entender específicamente qué es el *big data* cuando se trata de datos personales; los sujetos que ofrecen y tratan, analizando tanto los datos masivos como quienes los usan o aplican; y el papel que tendrá la responsabilidad demostrada al igual que la transparencia. Finalmente, se incluirán algunas conclusiones derivadas de las cuestiones previas.

I. LA REALIDAD DE LOS DATOS PERSONALES MASIVOS

Cuando los legisladores o, en su caso, autoridades reguladoras, han abordado la cuestión relativa a la protección de datos personales o la privacidad para promulgar normas o regulaciones, siempre lo han hecho pensando en cientos o, como mucho, miles de datos personales tratados en una base de datos, pero no siempre de millones de datos personales.

Al respecto, en su informe titulado *Protecting Consumer Privacy in an Era of Rapid Change*, la Comisión Federal de Comercio (Federal Trade Commission, FTC) de los Estados Unidos de América resume los comentarios recibidos y apunta que las empresas deberían cumplir con el marco de privacidad, salvo que solo manejasen (recabasen, mantuviesen o utilizasen) una cantidad limitada de datos personales no sensibles y que estos no se compartan con terceras partes. Y como parámetro de medida al respecto, apunta 5.000 personas a las que se refieran los datos personales (FTC, 2012, p. iv).

Es decir, estamos pasando de una realidad de pequeños tratamientos a otra en la que prevalecerán los tratamientos masivos y en la que aumentará, sobre todo, el uso o la aplicación de los resultados de estos últimos.

Es así que, frente a la actualidad, marcada claramente por leyes y regulaciones de protección de datos personales y privacidad pensadas para tratamientos *limitados* en todos los sentidos, el futuro requiere reflexionar sobre el

hecho de que las limitaciones actuales se convierten en obstáculos, si queremos beneficiarnos realmente de las posibilidades que ofrece el análisis de los datos masivos, al mismo tiempo que se establecen nuevas garantías efectivas que sirvan para promover la confianza de la persona en el tratamiento y uso de sus datos personales.

La referencia a tratamientos *limitados* se debe, entre otras razones, a que las leyes y regulaciones actuales en la materia centran la atención fundamentalmente en finalidades primarias, surgiendo habitualmente complicaciones interpretativas cuando la finalidad es diferente o independiente; también en datos personales que se obtienen principal y directamente de la persona a la que se refieren. Y en cuanto a las garantías para la persona, fundamentalmente la aproximación actual se basa en un esquema que pasa por el consentimiento informado, en ocasiones otorgado de manera expresa, en atención a una finalidad del tratamiento que puede estar obviando otros posibles usos de los datos personales. Dicho esquema, aunque puede ser válido para el entorno en el que fue planteado y desarrollado, puede resultar no ser el más adecuado para el futuro de la economía digital y la sociedad.

Es así que la realidad de los datos personales masivos es la de plantear la necesidad de un cambio de paradigma en lo que se refiere a la protección de datos personales y la privacidad que, en última instancia, requiere impulsar la adopción de normas robustas, claras y flexibles, en el sentido de adaptables, ya que fundamentalmente la falta de flexibilidad actual da lugar a situaciones de ineficiencia tanto al momento de aplicarlas como en lo relativo a su objetivo último, que es el de proteger a la persona titular de los datos personales. Esta finalidad, en concreto, es a la que se referían hace ya más de un siglo Warren y Brandeis, al llamar la atención sobre la necesidad de dar el próximo paso para proteger a la persona a la vista de las "recientes invenciones y métodos de negocio"[1] (1890).

No obstante, los datos masivos, en concreto su uso como resultado del tratamiento analítico, también tienen implicaciones en áreas tales como los seguros, la justicia, la salud, los préstamos, el consumo, etc. Es decir, los datos personales masivos son necesarios para el desarrollo y crecimiento de la economía digital basada en ellos, tanto si son personales como si no lo son, y la sociedad en general, que puede y debe beneficiarse de su uso.

En particular, los datos personales masivos significan que hemos entrado en una nueva fase. La revolución de los datos masivos está dando lugar a cambios sociales y económicos que requieren reflexionar sobre el valor que la sociedad da a sus derechos a la protección de datos personales y a la privacidad, así como el papel de las normas, leyes y regulación, junto

1. Traducción del original en inglés.

con la autorregulación, en materia de protección de datos personales y privacidad en sus términos actuales y puestas en perspectiva de cara al futuro.

En cualquier caso, se trata también de generar confianza, lo que va a requerir, como ha puesto de manifiesto el Foro Económico Mundial durante los últimos años, y como veremos más adelante, de una nueva aproximación respecto a la transparencia, la responsabilidad demostrada (*accountability*) y el empoderamiento del titular de los datos. En este sentido, hay que referirse también a los cambios que se han ido produciendo en varios instrumentos internacionales en materia de protección de datos y privacidad que, a su vez, son, en ocasiones, los referentes que siguen los países en el desarrollo y adopción de normas nacionales.

II. EL ESTADO DEL ARTE DE LOS INSTRUMENTOS INTERNACIONALES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Los datos personales masivos requerirán una aproximación diferente a la actual, lo que implica que deban seguirse altos estándares internacionales en materia de protección de datos personales, privacidad y ciberseguridad, si se quiere alcanzar una protección efectiva de la persona.

El primero al que hay que referirse, en virtud de su fecha de aprobación inicial, es a la Recomendación del Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), relativa a las Directrices que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales, adoptada el 23 de septiembre de 1980, que fue revisada en 2013 dando lugar a una versión actualizada.

La actualización mantuvo los principios básicos y entre las cuestiones relevantes a las que se puso atención están: introducir el principio de responsabilidad, las notificaciones de brechas de seguridad (*data security breach notification*), así como la necesidad de abordar la dimensión global de la privacidad a través de mejorar la interoperabilidad.

El hecho de haber introducido el principio de responsabilidad, aunque solo se hizo para el responsable del tratamiento, es uno de los pilares sobre los que se deberá desarrollar la protección de datos personales y la privacidad en las próximas décadas. Al respecto cabe señalar que la responsabilidad es también una cuestión clave en la normativa colombiana sobre protección de datos personales, que está promoviendo la autoridad de control, esto es, la Superintendencia de Industria y Comercio, a través de la Delegatura para la Protección de Datos Personales, dependencia que publicó en el 2015 la *Guía para la implementación del principio de responsabilidad demostrada (Accountability)*.

Otra de las actualizaciones importantes es la relativa a reforzar el cumplimiento (*enforcement)* en materia de privacidad y la cooperación entre autoridades de control.

El segundo instrumento internacional al que se debe prestar atención es el Convenio n.º 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscrito el 28 de enero de 1981. Este Convenio fue también objeto de revisión, y una de las principales novedades consistió en plantear la inclusión de un nuevo artículo 7 bis, relativo a la transparencia en el tratamiento de los datos personales. También preveía un nuevo artículo 8 bis, bajo el título Obligaciones adicionales, en el que hacía referencia a que tanto los responsables, como en su caso, los encargados del tratamiento, adoptaran las medidas apropiadas para cumplir con las obligaciones previstas en el Convenio y fueran capaces de *demostrar* a las autoridades de supervisión competentes, que el tratamiento de los datos personales bajo su control se hacían cumpliendo con las provisiones del Convenio.

Además, también a nivel internacional y por su trascendencia, cabe destacar el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC, por sus siglas en inglés), de 2004, que entre otros principios contempla el relativo a la responsabilidad, en virtud del cual el responsable del tratamiento deberá observar las medidas que permitan cumplir con los principios de la protección de datos personales previstos en dicho marco. Y en caso de que los datos sean transmitidos a terceras partes, nacional o internacionalmente, el responsable tendrá que obtener el consentimiento del titular de los datos personales, o actuar con la diligencia debida y adoptar medidas razonables para asegurar que el destinatario de los datos personales los proteja, consecuentemente con los principios de protección.

Sin perjuicio de estas actualizaciones, que son relevantes para los datos personales masivos, su tratamiento analítico así como la tecnología y otros servicios relacionados con la economía digital, hay que prestar atención específicamente a que el marco sobre la protección de datos personales y la privacidad sea el adecuado para proteger a la persona en sus derechos fundamentales; garantizar el libre flujo internacional de los datos personales; facilitar la innovación; evitar medidas proteccionistas arbitrarias o injustificables y, al mismo tiempo, impulsar la competitividad.

III. NI LA CANTIDAD DE DATOS PERSONALES NI LA CAPACIDAD DE SU ANÁLISIS: SU USO

El uso de los datos masivos y su tratamiento da lugar a importantes beneficios económicos y sociales, pudiendo citar, a modo de ejemplo, que la Comisión Europea (2014) ha indicado que el uso del *big data* por los cien fabricantes más importantes de la Unión Europea podría suponer ahorros de 425 billones de euros.

Pero, al mismo tiempo, la existencia de un riesgo por su mal uso es el centro de atención de las autoridades de protección de datos personales, como por ejemplo el Supervisor Europeo de Protección de Datos en la Unión Europea, e incluso los gobiernos, como ocurre en el caso de los Es-

tados Unidos de América, que ha publicado ya varios documentos relevantes sobre la materia, a los que se presta atención más adelante.

Esta consideración por diferentes autoridades puede deberse, fundamentalmente, al hecho de que el tratamiento analítico de los datos masivos va a implicar la necesidad de repensar algunos conceptos, como por ejemplo y en particular el de privacidad, así como la efectividad de algunos principios como los de información y consentimiento, sobre los que en un informe de la Casa Blanca (White House, 2014, p. xi) se indica: "El marco de la información y el consentimiento también se está convirtiendo en inviable como una base útil de política pública". Sobre los principios de protección de datos aplicados al *big data*, el International Working Group on Data Protection in Telecommunications (IWGDPT) ha afirmado que el *big* data supone un desafío.

Respecto a la ineficiencia del consentimiento, para Gil González (2016) resulta claro que "los retos surgidos del *big data* hacen que el consentimiento, por sí mismo, no sea suficiente" (p. 71) y "tal vez el modelo de consentimiento informado ya no deba ser la piedra angular del tratamiento de datos" (p. 122).

Lo anterior da lugar a la necesidad de considerar que deben impulsarse principios como los de transparencia y responsabilidad demostrada para conseguir una protección efectiva de la persona, especialmente en lo concerniente a sus derechos a la privacidad y a la protección de datos personales, por cuanto convergen en lo que respecta al control de la persona física sobre el tratamiento de sus datos personales.

Aunque en algún momento se utilicen indistintamente, privacidad y protección de datos personales no son lo mismo. El término privacidad es un concepto amplio que no tiene una definición concreta, debiendo considerar que, como se indica en el informe de la Casa Blanca, "abarca no solo el famoso 'derecho a ser dejado en paz', o mantener los asuntos o relaciones personales en secreto, sino también la posibilidad de compartir la información de forma selectiva pero no pública" (White House, 2014, p. xi).

Por su parte, el derecho a la protección de datos personales, desde una perspectiva europea, es un derecho fundamental consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que indica lo siguiente:

> Artículo 8
> Protección de datos de carácter personal
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Este derecho fundamental se articula sobre la base de unos principios para el tratamiento lícito y legítimo de los datos personales, unas obligaciones exigibles a quien los trata, así como unos derechos para el titular de los datos personales. Y también sobre la existencia de una autoridad de control o de supervisión independiente que vele por el cumplimiento de la normativa por parte de quienes, ya sean del sector privado o público, tratan los datos personales.

Se trata de un derecho específico, en el sentido de autónomo, que surge a partir del derecho a la intimidad.

Al efecto cabe recordar que el apartado 1 del artículo 1 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, indica:

> Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

En cualquier caso, el tratamiento analítico de los datos personales, mediante el uso de algoritmos, permite obtener modelos (*patterns*) y correlaciones (*correlations*) que pueden llegar a desvelar más datos sobre la persona. Incluso puede llegarse a dichos datos sin haberlos obtenido de la persona, sino de diversas fuentes, y combinarlos a través de la fusión de datos (*data fusion*).

Esto, unido al hecho de que en la actualidad la persona está dejando de ser, en muchas ocasiones, quien proporciona los datos, debido a que pueden obtenerse de diferentes fuentes y mediante el uso de sensores que los recaban de dispositivos, da lugar a que haya que prestar atención al futuro de la privacidad y la protección de datos personales, ya que la transparencia y la responsabilidad podrían ser los principios fundacionales de estas, así como las claves para generar la confianza necesaria en el tratamiento de los datos personales.

Los principios de transparencia y responsabilidad son aplicables a quienes tratan o usan datos personales, y el tratamiento analítico de los datos masivos requiere prestar atención a tales principios para generar la confianza necesaria por parte de todas las partes involucradas, ya sean las personas a las que se refieren los datos personales, las autoridades de protección de datos u otras.

Desde el punto de vista de la protección de datos personales y la privacidad, que los datos personales sean masivos, en el sentido de aplicables en gran cantidad, es un aspecto o incluso un criterio relevante a considerar en ciertos casos, pero no es el todo.

La atención debe ponerse, esencial y especialmente, en el uso de los datos personales que

resultan del tratamiento analítico y, sobre todo, en aquellos usos que pueden dar lugar a consecuencias negativas para las personas a las que se refieren, como, por ejemplo, la denegación de un crédito o la exigencia de una póliza de seguro más cara.

Al respecto hay que considerar también que, por escasos que pudieran ser, unos pocos datos personales, por su naturaleza, pueden proporcionar una información privilegiada sobre la persona a la que se refieren. Y los datos personales masivos, por sí solos, pueden no dar ninguna información, a menos que quien los analiza lo haga con el conocimiento necesario para poder hacer predicciones basadas en correlaciones. Y son las consecuencias, en particular las negativas, del uso que resulta de dicho análisis, que entra dentro del concepto de tratamiento, las que requieren de medidas para evitar intromisiones indebidas en la protección de datos personales y la privacidad o, incluso, que se produzcan discriminaciones, tal como ha apuntado el informe de la Executive Office of the President's Council of Advisors on Science and Technology (EOPCAST), al indicar que "el uso indiscriminado de estos análisis puede causar discriminación contra las personas o falta de equidad debido a la incorrecta asociación con un grupo determinado" (2014, p. 25), o también la Conferencia de Autoridades de Protección de Datos y Privacidad al observar en la Resolución sobre big data ya mencionada, que "el *Big Data* también puede usarse en formas que generan una preocupación importante respecto a la privacidad de las personas y los derechos civiles, y a las protecciones contra la discriminación y las vulneraciones al derecho a trato igual" (2014, p. 2). Además, esto implica que puedan vulnerarse otros derechos fundamentales de la persona, entre los que se encuentran la igualdad de trato e incluso su libertad.

El análisis de los datos masivos es el que permite, si se tienen además los conocimientos necesarios, desvelar lo que aquellos tienen que o pueden decir. Según la Conferencia de Autoridades de Protección de Datos y Privacidad "el Big Data implica una nueva forma de ver la información, revelando aquella que antes era difícil de extraer o que estaba oculta" (2014, p. 1).

Es decir, nos encontramos ante datos personales masivos y tratamientos analíticos, propiciados por la imparable y constante evolución de las tecnologías de la información. En el ya citado informe de la EOPCAST se señala:

> Los datos masivos son masivos en dos sentidos diferentes. Son masivos en cuanto a la cantidad y variedad de datos disponibles para su tratamiento. Y, son masivos en cuanto a la extensión del análisis (denominado "analítica") que puede ser aplicado a dichos datos, en última instancia para hacer las deducciones y sacar conclusiones.[2] (2014, p. ix).

2. Traducción del original en inglés.

El International Working Group on Data Protection in Telecommunications (IWGDPT), en su Documento de trabajo sobre datos masivos y privacidad, se refiere también a esta cuestión en palabras similares:

> Datos masivos es un término que se refiere al enorme aumento en el acceso y uso automatizado de la información. Se refiere a las cantidades gigantes de datos digitales controladas por las empresas, autoridades u otras grandes organizaciones que están sujetos a análisis extensivos basados en el uso de algoritmos. (2014, p. 1).[3]

Y cuando quien usa los resultados de dichos tratamientos analíticos de datos masivos lo hace con fines poco claros o de manera irresponsable, es cuando surge el riesgo de que su uso pueda materializarse en graves consecuencias para la persona.

Aunque la posibilidad de revelar información, que a primera vista podría no ser percibida, puede tener importantes implicaciones que es necesario tener en consideración, no es donde está el riesgo. La privacidad, en particular, incluye tanto la facultad de evitar la observación o mantener los asuntos y relaciones personales en secreto como la habilidad de compartir información selectivamente pero no de manera pública. En este sentido, el informe de la EOP-CAST sobre datos masivos y privacidad indica:

> El término "privacidad" abarca tanto evitar la observación, o mantener los asuntos y relaciones personales en privado, como la habilidad de compartir información de manera selectiva pero no públicamente. El anonimato se superpone con la privacidad, pero los dos no son idénticos. Votar es reconocido como algo privado, pero no anónimo, mientras que la autoría de un ensayo político puede ser anónimo, pero no es privado. (2014, p. 2).[4]

Por su parte, el derecho fundamental a la protección de datos personales puede concebirse como un derecho autónomo de la privacidad, en el sentido de la Unión Europea, de manera que implica el control sobre los datos personales. De nuevo, la atención específica debe ponerse en el uso que pueda darse a los datos personales.

Además de revelar información y en relación con dicha posibilidad, el tratamiento de los datos personales masivos permite identificar y predecir tendencias y correlaciones (IWGDPT, 2014, p. 3) que, en su caso, podrían dar lugar a crear un perfil de la persona a la que se refieren los datos personales o predecir su comportamiento. Pero, de nuevo, el riesgo no está en la capacidad de tratamiento ni en el perfil o la predicción sobre el comportamiento de la persona.

El riesgo está en el uso que se dé a los datos masivos una vez que han sido objeto de un tra-

3. Traducción del original en inglés.
4. Traducción del original en inglés.

tamiento analítico. Esto implica que deba plantearse cómo se protegerán, en su caso, los datos personales y la privacidad en la era de los datos personales y tratamientos masivos. Hay quién aboga porque la protección es más importante que nunca y que no se debería aceptar, en modo alguno, que los principios de la protección de datos personales y la privacidad que se han aplicado durante décadas a nivel internacional se vean mermados.

En particular, el IWGDPT opina:

> La protección de la privacidad es más importante que nunca en un momento en el que se incrementan las cantidades de información que son recabadas sobre las personas. Los principios de privacidad constituyen nuestra garantía de que no estaremos sujetos a perfilado extensivo en un arsenal cada vez mayor de nuevos contextos. Una merma de los principios de privacidad clave, en combinación con un uso cada vez más extensivo de los datos masivos, puede tener consecuencias adversas para la protección de la privacidad y otros valores sociales importantes tales como la libertad de expresión y las condiciones para el intercambio de ideas. (2014, pp. 1-2).[5]

Como se ha señalado, estos principios, en tanto que incluidos en varios instrumentos internacionales de referencia, entre los que se encuentran las Directrices de la OCDE, el Convenio 108 del Consejo de Europa y el Marco de Privacidad de APEC, son fundamentales y, junto con los derechos del titular de los datos personales y la ciberseguridad, delimitan el contenido nuclear de la protección de datos personales y la privacidad, si bien la aproximación que se propone a los datos personales masivos y tratamientos analíticos, como a cualquier otra cuestión, debe partir de la responsabilidad, la transparencia y la búsqueda de un instrumento global, que lejos de la rigidez de las normas legales actuales permita satisfacer las necesidades de todas las partes implicadas.

Es decir, no se trata ni de los datos personales masivos ni de su tratamiento intensivo o analítico, que son parte de un todo, sino de comprender que el futuro de la protección de datos personales y la privacidad pasa por impulsar medidas que tengan en consideración la realidad y partan de las lecciones aprendidas. Más que de la cantidad o el volumen de datos personales se trata del uso de estos, en particular, cuando se produce un mal uso, lo que requiere que haya que promover, a través de los instrumentos adecuados, la transparencia y la responsabilidad demostrada de quienes los tratan, al mismo tiempo que se desarrolla una labor de concienciación de los titulares de los datos respecto del significado de su derecho fundamental a la protección de datos personales.

Entre otras, estas lecciones implican que se deban tener en consideración las diferentes aproximaciones que pueden encontrarse a la protección de datos personales y la privacidad,

5. Traducción del original en inglés.

para así buscar de manera comprometida, por todas las partes implicadas, instrumentos adecuados y adaptables en materia de protección de datos personales y privacidad.

IV. SUJETOS QUE OFRECEN O TRATAN DATOS PERSONALES MASIVOS Y LAS RELACIONES ENTRE ESTOS

La responsabilidad del cumplimiento, con independencia de cuál sea el instrumento aplicable en materia de protección de datos personales y privacidad, es exigible a uno o a varios sujetos, dependiendo de cada situación. Y en el caso de los datos masivos y tratamientos analíticos no hay diferencia, a pesar de que pueden darse relaciones jurídicas que requieren asegurar el cumplimiento a lo largo del ciclo de vida de los datos personales. Este ciclo de vida es también la cadena de valor (*value chain*) de los datos personales masivos, en la que pueden participar múltiples sujetos entre los que se incluyen, por ejemplo, los recolectores de los datos personales, quienes los analizan y quienes los usan.

En relación con los tratamientos masivos de datos, en la práctica siempre habrá uno o varios responsables, siendo una de las cuestiones relevantes a considerar el hecho de que la recolección y el análisis de los datos personales masivos dan lugar a nuevas oportunidades de negocio, que consisten en el licenciamiento de cantidades de datos personales, lo que puede llevar a situaciones de transferencia, nacional o internacional, así como de corresponsabilidad. Y esto sin perjuicio de que, en su caso, el encargado del tratamiento tenga que cumplir también con las obligaciones que le son exigibles en materia de protección de datos personales.

A. Responsables del tratamiento en los sectores público y privado

En particular, los responsables del tratamiento analítico de datos personales masivos pueden ser tanto del sector público como del privado y, en cualquier caso, serán también, de alguna forma, parte de la cadena de valor de los datos personales masivos.

Al respecto, el IWGDPT ha indicado que "una amplia cadena de partes interesadas están involucradas a lo largo de la cadena de valor de los datos masivos (...) Algunas partes interesadas están involucradas solo en partes de esta cadena de valor".[6] (2014, p. 5).

En el caso específico del sector público, dadas las atribuciones que este tiene, se ha convertido en un importante proveedor de datos masivos, debiendo destacar al respecto la tendencia hacia los datos abiertos (*open data*).

En este sentido, cabe destacar el hecho de que el país cuenta con una Estrategia de Datos Abiertos, y en los *Lineamientos para la implementación de datos abiertos en Colombia*,

6. Traducción del original en inglés.

publicados por el Ministerio de Tecnologías de la Información y las Comunicaciones, se prevé como una de las excepciones a la reutilización la relativa a "aquellos relacionados con los datos personales cuya divulgación pueda atentar contra los derechos de privacidad e intimidad de las personas" (2011, p. 11).

El acceso a los datos abiertos lleva a considerar la reutilización de los datos, personales o no, que con carácter general se produce, según el Grupo de trabajo del artículo 29 de la Directiva 95/46/CE (GT 29), en los siguientes términos:

> 1) Poner a disposición del público bases de datos completas;
> 2) En un formato electrónico estandarizado;
> 3) A cualquier persona, sin llevarse a cabo un proceso de examen previo;
> 4) Sin sujeción al pago de una tasa o cantidad, y
> 5) Para el uso con fines comerciales o no conforme a una licencia abierta. (2013, p. 35).

En paralelo, en el sector privado, desde hace unos años están cobrando especial relevancia los denominados corredores de datos (*data brokers)*, que pueden actuar como recolectores y acumuladores de datos personales, pudiendo incluso tratarlos en algunos casos, combinando datos personales obtenidos de diversas fuentes electrónicas en línea (*online*) o no (*offline*), para ofrecer a otros el resultado de dichos tratamientos. Cabe señalar que, con respecto a los *data brokers*, la FTC en Estados Unidos ha propuesto adoptar medidas normativas enfocadas a la transparencia y a la responsabilidad (2014, p. 57).

En cuanto a quienes tratan datos personales masivos, los responsables tienen que adoptar e implementar las medidas necesarias para asegurar el cumplimiento de los principios y deberes aplicables al tratamiento de estos, las medidas para atender los derechos de los titulares de los datos personales, así como velar por la seguridad de los datos personales, considerando, en particular, la ciberseguridad.

Y es, precisamente, el principio de responsabilidad, que se prevé en la normativa colombiana sobre protección de datos personales y que fomenta también la autoridad de control, el que puede dar las respuestas necesarias con respecto al futuro de la protección de datos personales y la privacidad.

B. Relaciones entre los sujetos que ofrecen y tratan datos personales masivos

Como ya se ha indicado, en particular en relación a la posibilidad de reutilización de los datos abiertos del sector público, se dan casos en los que dicha reutilización se hace conforme a licencias abiertas.

Dichas licencias, en el caso del uso de datos personales, deben considerarse también a la vista de la transferencia de datos personales entre dos responsables del tratamiento, la

cual según el artículo 3.4 del Decreto 1377 de 2013:

> Tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

A su vez, la transmisión de datos entre un responsable y un encargado del tratamiento es definida en el artículo 3.5 del Decreto 1377 de 2013, como el "tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable."

Junto a lo anterior, el hecho de que haya, o pueda haber, una cadena de valor, debería implicar que se asegure a lo largo de esta el cumplimiento de unos principios básicos que, a la larga, permitan garantizar el derecho fundamental a la protección de datos personales y a la privacidad, cuando los datos masivos tratados sean personales. Se busca así que la transparencia y la responsabilidad demostrada por todas las partes implicadas, sean o no responsables del tratamiento, encargados del tratamiento u otras, queden garantizadas a lo largo de toda la cadena y el ciclo de vida de los datos personales, lo que permitirá también impulsar la confianza necesaria. Más allá de la protección de datos personales, la transparencia y la responsabilidad demostrada son comunes a cualquier otra área de actividad o actuación.

Es decir, garantizar la transparencia y la responsabilidad demostrada requiere también adoptar medidas en las relaciones jurídicas que se puedan dar entre las diferentes partes que intervengan en la cadena de valor de los datos personales masivos. Conseguir un alto nivel de protección de datos personales y privacidad requiere, en buena medida, asegurar que los datos personales son tratados conforme a altos estándares de transparencia y responsabilidad. Además, incluir y mantener, en la medida en que corresponda, estas garantías a lo largo de toda la cadena de valor o ciclo de vida de los datos personales permitiría, al mismo tiempo, mitigar riesgos en relación con la posible re-identificación del titular de los datos personales, aspecto considerado por el IWGDPT como uno "de los mayores riesgos asociados con el análisis de los datos masivos" (2014, p. 7), ya que la anonimización, por sí sola, podría no ser eficiente.

Y también afirma el IWGDPT:

> Desafortunadamente, cada vez es más fácil superar a la anonimización a través de las muchas técnicas que están siendo desarrolladas para muchas aplicaciones legítimas de datos masivos. En general, como el tamaño y la diversidad de los datos disponibles crece, la probabilidad de ser capaz de re-identificar a las personas (es decir, asociar de nuevo sus registros con sus nombres) crece considerablemente. (2014, p. 7).

Complementar las soluciones tecnológicas disponibles en cada momento con otras so-

luciones no tecnológicas como la autorregulación, podría ayudar también a evitar riesgos para la protección de datos personales y la privacidad.

No se trata de regular más, considerando como indica Rodotà, que "vivimos ya en una *law-saturated society*, una sociedad repleta de derecho, de reglas jurídicas de las más variadas procedencias, dictadas por los poderes públicos o privados, con una intensidad que evoca no tanto una necesidad como una imparable deriva" (2010, p. 25), sino más bien, de adoptar medidas adecuadas basadas en la transparencia, en la responsabilidad demostrada, que a su vez sean interoperables en un escenario global. Dichas medidas adecuadas deben permitir un buen gobierno, así como la posibilidad de exigir la rendición de cuentas.

V. TRANSPARENCIA

La transparencia, entendida como la traducción de los términos *openness* o *transparency,* es un principio incluido en varios instrumentos internacionales en materia de protección de datos personales y privacidad a los que ya se ha hecho referencia, por ejemplo, las Directrices de la OCDE y el Convenio 108, en particular como consecuencia de la revisión llevada a cabo en el caso de este último.

La falta de transparencia en materia de protección de datos personales genera desconfianza y, por lo tanto, puede ser fuente de malentendidos y litigios.

En este sentido, el IWGDPT ha indicado:

> La falta de transparencia e información sobre cómo recaban y usan los datos puede implicar que seamos presa de decisiones que no entendemos y sobre las que no tenemos ningún control. (...) La mayoría de las personas no están familiarizadas con muchos de los jugadores que operan en este mercado, especialmente con los corredores de datos ("data brokers") y las compañías de análisis. (2014, p. 10).[7]

Es por ello que resulta necesario aumentar el nivel de transparencia cuando se tratan datos personales, especialmente si hay datos personales sensibles.

No se trata solo del principio de información o de la información necesaria para que el titular de los datos personales pueda ejercer sus derechos, sino de transparencia sobre las prácticas que se siguen en materia de protección de datos personales y privacidad, de manera que las personas a quienes se refieran los datos personales puedan saber qué prácticas se siguen en el tratamiento y, en particular, para qué se usan.

Además, la transparencia facilitará saber quién interviene, o no, en la cadena de valor y el ciclo de vida de los datos personales, lo que, a su

7. Traducción del original en inglés.

vez, posibilitará al titular de estos el ejercicio de sus derechos, y a las autoridades competentes, ya sea el órgano de control, una autoridad reguladora o judicial, exigir la responsabilidad que corresponda. Lo anterior sin perjuicio de que dicha responsabilidad sea exigible en virtud de una norma legal o regulatoria, o incluso de un instrumento autorregulatorio. En este último caso cabría considerar también quién tiene atribuida la potestad de velar por su cumplimiento, así como su potestad sancionadora, siendo dichas facultades fundamentales para garantizar la eficiencia de dicho instrumento.

En cualquier caso, la transparencia aumentada servirá para estimular la confianza necesaria en todas las partes involucradas, desde las personas cuyos datos son objeto de tratamiento y uso hasta las autoridades de supervisión o reguladoras competentes, evitando así medidas legislativas innecesarias que únicamente supongan una carga, y una señal de que no se ve con nitidez la realidad.

VI. RESPONSABILIDAD DEMOSTRADA

Como concepto, al igual que ocurre con otros traducidos del inglés, el de responsabilidad (*accountability*) es difícil de concretar debido a las diferentes percepciones que pueden tenerse.

Al respecto el GT 29 aclara:

> El término «responsabilidad» (*accountability*) proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aunque la definición exacta de «responsabilidad» resulta compleja en la práctica. Pero de forma general, el término apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse. Competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza. (2013, p. 8).

La responsabilidad, como principio aplicable al tratamiento de datos personales, no es un concepto nuevo ni exclusivo de esta área. No obstante, en los últimos años se han intensificado las referencias a este en diferentes instrumentos internacionales sobre privacidad y protección de datos personales, como por ejemplo las Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, lo que muestra la importancia de asegurar que quienes tratan los datos personales adopten e implementen medidas efectivas, lo que sin duda dará lugar a un cambio de paradigma y aproximación a la protección de la persona en lo que se refiere a sus datos personales. Es, quizás en este momento, el siguiente paso a dar para proteger a la persona, al que Warren y Brandeis se refirieron ya en su trascendental artículo “The Right to Privacy”, publicado en 1890.

Esta tendencia a impulsar el principio de responsabilidad es una de las claves para el futuro de la protección de la persona, en lo que se refiere al tratamiento de sus datos personales. Buena muestra de ello es el hecho de que Co-

lombia también ha previsto este principio en la normativa sobre protección de datos, dedicándole en el Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012, el capítulo VI, artículos 26 y 27.

Además, como ya se ha mencionado, la Superintendencia de Industria y Comercio, como autoridad garante o de control, publicó en 2015 una *Guía para la implementación del principio de responsabilidad demostrada (Accountability)*. Una de las cuestiones específicas a las que se refiere esta guía es la relativa a los riesgos asociados al tratamiento de datos personales, incidiendo en la necesidad de que el responsable del tratamiento administre dichos riesgos, considerando específicamente, más que la cantidad, los "tipos de datos personales tratados", lo que obviamente es aplicable en el caso de los datos masivos.

Que el tratamiento analítico sea de datos personales masivos no significa que exista un riesgo en todos los casos, ya que la atención debe ponerse en el tipo o la naturaleza de los datos personales y los riesgos que podría conllevar su uso, en concreto, su mal uso, para la persona.

Unido a lo anterior, el concepto de dato personal en varias legislaciones sobre protección de datos personales alrededor del mundo es muy amplio, lo que en la práctica implica que puedan darse situaciones de divergencia, especialmente si se compara la legislación de la Unión Europea y de varios países de Latinoamérica con el marco aplicable en el caso de Estados Unidos. Esto muestra la necesidad de encontrar un equilibrio, siendo una oportunidad el hecho de seguir estándares internacionales, como por ejemplo, la norma ISO 19944 relativa a los flujos de datos en y entre dispositivos y servicios de nube.[8]

Reducir las diferencias entre las distintas percepciones de qué es y no es un dato personal es relevante y conveniente.

VII. ATENDER AL PASADO PARA AVANZAR EN EL FUTURO DE LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS APLICABLES AL *BIG DATA*

El uso que pueda darse a los tratamientos de datos personales, con independencia de que dichos tratamientos sean analíticos e intensivos o no, y los datos personales sean masivos o no, es lo realmente importante. Y es sobre el uso que pueda darse a los datos personales donde hay que adoptar medidas, si se quiere proteger realmente a la persona.

Es necesario también prestar atención a los importantes cambios que se están produciendo como consecuencia de los avances tecnológicos, y que cada día implican que muchas normas y los esquemas en los que estas se basan queden obsoletos, resultando por tanto ineficientes para ofrecer una protección efectiva. En este sentido, por ejemplo, pueden darse

8. Norma publicada en septiembre de 2017.

situaciones en las que no es la persona quien proporciona sus datos personales, sino que son recabados de dispositivos.

Tal como indica la EOPCAST en el Report to the President, *Big Data and Privacy: a technological perspective:*

> Controlar el acceso a los datos personales una vez que dejan de estar en posesión exclusiva de la persona se ha visto históricamente como un medio de controlar el daño potencial. Pero hoy en día, los datos personales pueden no estar, o no haber estado, en posesión de la persona —por ejemplo, pueden ser recabados de manera pasiva a partir de fuentes externas, tales como cámaras públicas y sensores—, o sin su conocimiento, a través de divulgaciones públicas electrónicas hechas por otras personas que utilizan los medios de comunicación social. Además, los datos personales pueden ser derivados de poderosos análisis de datos (...) cuyo uso y la producción son desconocidos para el individuo. (2014, p. 5).[9]

Por lo tanto, es necesario atender al pasado, a lo ya aprendido, considerando qué esquemas han resultado o están resultando ser ineficientes tanto desde el punto de vista de los instrumentos aplicados como de los principios sobre los que, hasta la fecha, se ha basado la protección de los datos personales para, sobre esta base, avanzar en el futuro de la protección de datos personales y la privacidad.

La anonimización o disociación de los datos personales, debido al estado de la tecnología, ha dejado de ser suficiente y, por tanto, no puede generar una expectativa de privacidad suficiente.[10] Según la EOPCAST (2014), "la anonimización está siendo superada cada vez de forma más fácil por las varias técnicas que están siendo desarrolladas para muchas aplicaciones legítimas de los datos masivos" (p. xi), aunque "sigue siendo útil como una protección adicional, pero no es robusta contra el futuro próximo de los métodos de re-identificación" (p. 39).[11]

Es decir, a corto plazo la anonimización será un *plus* o valor añadido (*add-on*) para la privacidad y la protección de datos personales, pero no la técnica que proporcione una solución ni única ni definitiva cuando quiere, por diferentes motivos legítimos, mantenerse oculta la identidad, o simplemente preservarse sin motivo alguno.

Por su parte, el GT 29 en el Dictamen 5/2014 sobre técnicas de anonimización advierte:

> Los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados. Efectivamente, por una parte, la anonimización y la reidentificación son campos de investigación

9. Traducción del original en inglés.
10. Traducción del original en inglés.
11. Traducciones del original en inglés.

> activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. En suma, la anonimización no debe contemplarse como un procedimiento esporádico, y los responsables del tratamiento de datos han de evaluar regularmente los riesgos existentes. (2014, p. 4).

Además, hay que considerar que las "técnicas de anomización más robustas, por sí solas, no solucionarán los retos que plantean los datos masivos a la privacidad. Es necesario que haya soluciones adicionales" (IWGDPT, 2014, p. 16).

Y dicho futuro requiere, entre otras muchas cosas, de normas robustas y claras en cuanto a qué usos de los datos personales están permitidos o no, debiendo ser al mismo tiempo normas adaptables, de manera que permitan responder eficazmente, sin quedar rápidamente obsoletas. Al mismo tiempo, también "es necesario fortalecer la cooperación internacional" (Remolina, 2015, p. 378), lo que quizás pueda conseguirse si los países consideran la adopción de altos estándares en materia de protección de datos personales y privacidad, conforme a convenios u otros instrumentos internacionales, así como al desarrollo de las atribuciones que tienen conferidas en la materia las autoridades de protección de datos personales.

En relación con lo anterior, lo fundamental es que tanto si se trata de la revisión de normas ya vigentes como de adoptar nuevos instrumentos, se tenga en consideración que los principios de responsabilidad y transparencia son esenciales, y además constituyen una oportunidad a nivel internacional, ya que plantean menos problemas de interpretación que otros principios sobre los que puede haber importantes divergencias.

El tratamiento analítico de los datos masivos plantea, por tanto, la necesidad de repensar cómo aplicar principios normativos o autorregulatorios, y usar la tecnología para generar y mantener la confianza necesaria en el uso de los datos personales o de la información personal. Se trata de garantizar a la persona el control sobre el uso de sus datos, superando, en cierta medida, que la privacidad signifique siempre mantener cierta información en secreto (Richards y King, 2014, p. 16), así como prestar más atención a cuando los datos personales no son proporcionados por el propio interesado, para facilitarle en cualquier caso el control sobre estos.

VIII. CONCLUSIONES

En el caso de los tratamientos analíticos de los datos masivos, el riesgo para la persona respecto a su privacidad y la protección de sus datos personales no está tanto en la obtención o el tratamiento, sino en el uso que se dé al resultado de dicho tratamiento y las consecuencias que este pueda tener para dicha persona.

El tratamiento analítico de datos personales masivos es una buena oportunidad para con-

seguir el máximo beneficio social y económico de los avances tecnológicos, si bien es necesario prestar atención al uso que pueda hacerse de aquellos para evitar intromisiones en la privacidad y vulneraciones a la protección de datos personales que supongan consecuencias negativas tales como la discriminación, del tipo que sea, o, en última instancia, afecten incluso la libertad misma de la persona.

Además, este avance tecnológico implica también que deban revisarse esquemas relativos a la protección de la privacidad y de los datos personales, que han quedado obsoletos, y que requieren evaluar, entre otras cuestiones, la efectividad de los principios que han venido aplicándose hasta la actualidad, tales como la información y el consentimiento (*notice and consent)* para el tratamiento de datos personales. También el uso de técnicas como la anominización, que por sí solas resultan ahora insuficientes ante el vertiginoso avance tecnológico de técnicas de re-identificación y su aplicación a los datos personales masivos.

Desde el punto de vista de los principios aplicables, el futuro de la privacidad y la protección de datos personales está en impulsar, fundamentalmente, la transparencia y la responsabilidad. La privacidad y la protección de datos son claves para generar la confianza, de manera que la transparencia en las prácticas sobre el uso de los datos personales y la responsabilidad demostrada serán el estándar en los próximos años. Esto llevará a dar un paso definitivo frente a esquemas actuales enfocados en la "privacidad por consentimiento", de manera que la privacidad y la protección de datos estarán basadas en la transparencia y la responsabilidad.

En la medida en que la privacidad y la protección de datos personales convergen en el control de la persona sobre sus datos personales, son necesarias la transparencia y la responsabilidad aumentadas. Seguramente el alcance de los conceptos de privacidad y protección de datos personales cambiarán en un futuro próximo, para evolucionar y seguir siendo un elemento esencial en materia de confianza.

Para que la transparencia y la responsabilidad aumentadas sean principios efectivos, reduciendo en la medida de lo posible el riesgo de cuestionamientos como ha ocurrido en el caso de otros principios, es necesario pensar también en contar con normas robustas, claras en cuanto a qué uso de los datos personales está permitido y dónde están los límites, así como adaptables. Dichas normas no deben girar en torno al cómo (¿cómo son los datos personales?, ¿cómo se tratan los datos personales?, ¿cómo...?) sino al qué (¿qué principios serán efectivos a largo plazo?, ¿qué medidas deberían adoptar quienes tratan datos personales para cumplir con los principios de transparencia y responsabilidad?, ¿qué criterios considerar para evaluar el riesgo que implica un tratamiento de datos personales?, ¿qué...?).

Y sobre todo, atender al pasado. Por ejemplo, Warren y Brandeis en su artículo "The Right to Privacy", publicado en 1890, ya llamaban nuestra atención sobre el próximo paso que debe darse para proteger a la persona. Dicha protec-

ción permitirá generar y mantener confianza en el uso de los resultados de los tratamientos analíticos de datos masivos, lo que a largo plazo determinará poder contar con un marco adecuado para innovar en busca de la próxima revolución tecnológica, con un alto grado de seguridad jurídica para todas las partes implicadas.

En definitiva, si aplicásemos el actual marco regulatorio de la protección de datos personales y privacidad a los datos masivos y su tratamiento analítico alrededor del mundo, el resultado del análisis nos llevaría a poder afirmar que es necesario un cambio de aproximación, y que en lugar de complejas regulaciones nacionales, por ser en unos casos excesivamente prolijas y en otros demasiado prescriptivas, o incluso ambas a la vez, se impulse decidida y definitivamente, a nivel internacional, el principio de responsabilidad, a través de normas robustas y adaptables que sean capaces, por una parte, de responder a la evolución social, tecnológica, económica y jurídica, lo que pasa por impulsar también la autorregulación, y, por otra parte, que faciliten también la innovación.

Referencias

1. Comisión Europea. (2014). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Hacia una economía de los datos próspera*. Recuperado el 27 de abril de 2017, de ec.europa.eu: http://ec.europa.eu/transparency/regdoc/rep/1/2014/ES/1-2014-442-ES-F1-1.Pdf

2. Executive Office of the President's Council of Advisors on Science and Technology [EOPCAST]. (2014). *Big Data and Privacy: A Technological Perspective*. *Report to the President.* Recuperado el 27 de abril de 2017, de obamawhitehouse.archives.gov: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

3. Federal Trade Commission. (2012). *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for businesses and policymakers*. Recuperado el 27 de abril de 2017, de ftc.gov: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

4. Federal Trade Commission. (2014). *Data brokers: A call for transparency and accountability*. Recuperado el 27 de abril de 2017, de ftc.gov: www.ftc. gov/system/files/documents/reports/data-brokers-call-transparency-accountabilityreport-federal-trade-commission-may-2014/140527databrokerreport. Pdf

5. Gil González, E. (2016). *Big Data, privacidad y protección de datos*. Madrid: Agencia Española de Protección de Datos/Agencia Estatal Boletín Oficial del Estado.

6. Grupo de trabajo del artículo 29 de la Directiva 95/46/CE [GT 29]. (2013). *Opinion 3/2013 on purpose limitation*. Recuperado el 27 de abril de 2017, de ec.europa.eu:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

7. Grupo de trabajo del artículo 29 de la Directiva 95/46/CE. (2014*). Dictamen 5/2014 sobre técnicas de anonimización*. Recuperado el 27 de abril de 2014, de ec.europa.eu: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

8. International Telecommunications Union. (2013). Big Data: Big today, normal tomorrow. *ITU-T Technology Watch Report*.

9. International Working Group on Data Protection in Telecommunications [IWGDPT]. (2014). *Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics*. 55th Meeting, 5-6 May 2014, Skopje, Macedonia.

10. Mayer-Schönberger, V. y Cukier, K. (2013). *Big Data: la revolución de los datos masivos*. Madrid: Turner Publicaciones.

11. Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (23 de septiembre de 1980). *Recomendación del Consejo Relativa a las Directrices que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales*. Obtenido de http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

12. Remolina Angarita, N. (2015). *Recolección Internacional de datos personales: un reto del mundo post-Internet*. Madrid: Agencia Española de Protección de Datos/Agencia Estatal del Boletín Oficial del Estado.

13. Richards, N. M. y King, J. H. (2014). *Big Data and the Future for Privacy*. Recuperado el 27 de abril de 2017, de ssrn.com: http://ssrn.com/abstract=2512069

14. Rodotà, S. (2010). *La vida y las reglas. Entre el derecho y el no derecho*. Madrid: Trotta.

15. Supervisor Europeo de Protección de Datos. (2014*). Preliminary Opinion of the European Data Protection Supervisor. Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. Recuperado el 27 de abril de 2017, de edps.europa.eu: https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf

16. Warren, S. D. y Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220. Recuperado el 27 de abril de 2017, de groups.csail.mit.edu: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

17. White House. (2014). *Big Data: seizing opportunities, preserving values*. Estados Unidos de América*:* Executive Office of the President. Recuperado el 27 de abril de 2017, de obamawhitehouse.archives.gov: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf