Título: Big Data: riesgos y desafíos en el tratamiento masivo de datos personales
Autores: González Allonca, Juan Cruz - Ruiz Martínez, Esteban
Publicado en: LA LEY 08/04/2016, 08/04/2016, 1 - LA LEY2016-B, 1051
Cita Online: AR/DOC/373/2016

Sumario: I. Introducción.— II. Características del Big Data.— III. Big Data en el contexto de Internet de las Cosas y Cloud Computing.— IV. Riesgos de la actividad.— V. La aplicación de la ley 25.326 a las actividades de Big Data.— VI. Calidad del dato.— VII. Disociación de datos.— VIII. No automaticidad.— IX. Derecho de oposición.— X. Recomendaciones para un tratamiento seguro.— XI. Conclusiones.

El debilitamiento de los principios clave de privacidad junto con un mayor uso del Big Data es probable que tengan consecuencias adversas para la protección de la privacidad y de otros derechos fundamentales. Por ello los proveedores de estos servicios deberán estar atentos a respetar el principio de especificación de finalidad; limitar la cantidad de información recolectada y almacenada a un nivel que sea necesario para el propósito legítimo que pretende; solicitar el consentimiento del titular de los datos en relación con el uso de información personal para fines de análisis y de creación de perfiles; y si la información recolectada es transferida a terceros, deberá informarse de forma adecuada al titular del dato.

I. Introducción

La actividad informativa actual, desarrollada a través de la informática aplicada a dispositivos e Internet, está convirtiendo la realidad concreta en virtual, reflejando a las personas como un conjunto complejo de datos, conformando un "yo virtual" de gran trascendencia a los fines relacionales, en particular para la actividad económica del individuo.

Los medios informativos, a través de sus sistemas organizados de tratamiento de datos personales, pueden fácilmente invadir ámbitos sagrados de la persona que hasta hace poco eran inaccesibles, como, por ejemplo, su intimidad. Esto exige determinar un equilibrio entre dos institutos vitales de nuestro Derecho, que confluyen en el acto informativo: la libertad de información y los derechos del titular del dato.

Los medios informativos pretenden saber lo más posible sobre las personas, mientras que el titular del dato pretende ejercer libremente y sin interferencias todas sus libertades. En esta hipótesis de conflicto es cuando los derechos de la persona delimitan las facultades del medio informativo, pues la persona no puede ser un objeto de conocimiento, sino solo en aquello que otras personas y el Estado tienen también derecho a conocer sobre ella.

Es una realidad indiscutible que los distintos medios tecnológicos hoy vigentes detectan en tiempo real la ubicación de las personas y sus movimientos, como también sus gustos, consumos y navegación en Internet. Este tratamiento de su información personal es una clara injerencia en sus derechos a estar solo y a auto determinar su información personal. En tal sentido, hoy más que nunca debe reconocerse el derecho de las personas a no ser detectadas y/o seguidas, y/o controladas en sus consumos y demás actos, salvo que presten su consentimiento con carácter previo.

A lo antedicho se suma que, en forma reciente, la actividad informativa ha dado otro salto cualitativo, a través del desarrollo de la tecnología conocida como Big Data, que tiene por objeto el análisis de enormes cantidades de datos, estructurados o no. Esta tecnología realiza el tratamiento de datos con complejos algoritmos que permiten obtener nueva información sobre las personas, y que muchos anticipan que se convertirá en una herramienta clave del desarrollo, sustentando nuevas olas de crecimiento en la productividad, innovación y excelencia.

Interesa aquí determinar sus características más relevantes a los fines jurídicos y proponer pautas de licitud frente a los derechos de la persona, en particular, el derecho a la intimidad y la protección de los datos personales.

II. Características del Big Data

Son características definitorias de la actividad del Big Data el tratar información en grandes volúmenes, utilizando la totalidad de los datos disponibles (variedad), y a altas velocidades (indispensable, dada la magnitud de la información). Estas características del Big Data son conocidas como "las tres V": volumen, variedad y velocidad; para lo cual se requiere el desarrollo y la utilización tanto de hardware como de software específicos.

Resulta de interés para este análisis, entonces, que el Big Data permite obtener de ciertas actividades de tratamiento de datos personales -conexiones de equipos a redes (ej. telefonía), navegación en sitios o redes sociales en Internet, etc.- múltiples conclusiones sobre las conductas de los individuos, por ejemplo, señalar su proclividad a determinadas acciones, o establecer índices de probabilidad sobre estados y situaciones del sujeto

(económicas, de salud, etc.), y determinar así la toma de decisiones por parte de los actores económicos del mercado. Debido a su velocidad, el uso de Big Data ha ayudado a obtener, en un breve lapso de tiempo, conclusiones que por los medios tradicionales hubiera tomado meses, permitiendo ágilmente que el analista de datos pueda cambiar sus ideas basándose en el resultado obtenido y volver a procesarlos hasta encontrar el resultado esperado.

III. Big Data en el contexto de Internet de las Cosas y Cloud Computing

Como se dijo, el impulso de Big Data trae aparejado beneficios económicos y sociales y, a su vez, genera un desafío en términos de privacidad y protección de datos personales. Ahora bien, el desarrollo de Big Data se da en un contexto marcado por rápidos avances tecnológicos, de los cuales mencionaremos dos, que se destacan por su alcance y por la complementariedad que los une con Big Data, ellos son: Internet de las Cosas o Internet of Thing (IoT) y los servicios de Cloud Computing.

Internet de las Cosas es un concepto que se refiere a la conexión de objetos cotidianos a Internet. Como Señala Segura,

La base de la IdlC es dotar a los dispositivos de la capacidad de observar, identificar y entender el mundo real sin la participación (ni la limitación) de una persona. (...) Se trata, en definitiva, de protocolos, sistemas y dispositivos interconectados con la capacidad de observar el mundo, generar información y de hablarse entre sí sin la intervención de una persona. Conforman una red con la capacidad de tomar información del ambiente y generar decisiones basadas en ese análisis (1) .

Según un estudio realizado por la empresa de equipos de telecomunicaciones Cisco Systems, en 2012 había 8.700 millones de objetos conectados a Internet, hoy esta cifra alcanza los 25.000 millones y, en 2020, habrá más de 50.000 millones; es decir, 6,58 dispositivos conectados a Internet por cada habitante de la Tierra (2). Esto se traduce en un flujo descomunal de datos (muchos de ellos de carácter personal), que redunda en un gran desafío para la industria, gobiernos y usuarios, a la hora de su gestión y protección.

El alcance de los productos y servicios que integrarán la IoT son innumerables y abarcan múltiples ámbitos. Resulta imposible, por ende, agotarlos en un listado; de modo que mencionaremos solo aquellos que tendrán un impacto destacable en la vida cotidiana de las personas.

La domótica, o automatización de las casas, permite, por ejemplo, que heladeras inteligentes conectadas a Internet controlen el stock de productos y realicen pedidos a supermercados digitales; el control de la temperatura y humedad de los hogares a través de termostatos inteligentes, cámaras IP y cerraduras online, entre algunos de los beneficios.

Otros de los usos es la wearable computing: la integración entre los dispositivos y la vestimenta y accesorios, para medir signos vitales. Prendas capaces de monitorear las condiciones climáticas y las preferencias del usuario, y adaptarse al ambiente para ser más o menos abrigados, más o menos impermeables.

Los automóviles conectados también harán uso de IoT, a través de la conducción automatizada y servicios a bordo. Según un estudio de Gartner (3), para el año 2020 circularán en el mundo más de 250 millones de autos conectados a Internet.

Las denominadas smart cities, que implica la automatización de las ciudades a través de sensores que, por ejemplo, controlen el tránsito y que automáticamente modifiquen la duración de los semáforos para facilitar su fluidez. También el monitoreo automático del alumbrado público, con el fin de aumentar el ahorro de energía.

En virtud de lo expuesto, IoT se proyecta como uno de los principales proveedores de información que alimentarán a las grandes bases de datos utilizadas en Big Data, tanto por su despliegue y variedad de dispositivos conectados, como por su capacidad de capturar y transmitir grandes volúmenes de datos.

Consideraremos ahora la otra de las variables tecnológicas clave que se conjugan con Big Data: Cloud Computing. Los servicios de cómputo por demanda a distancia, que comúnmente se denomina cómputo en la nube o Cloud Computing se refiere a un nuevo esquema en el uso de los recursos tecnológicos y de los modelos de consumo y distribución de esos recursos. El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos y su laboratorio de tecnología de información definieron este nuevo concepto de la siguiente manera:

Cloud Computing es un modelo para habilitar acceso conveniente por demanda a un conjunto compartido de recursos computacionales configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios. Este modelo de nube promueve la disponibilidad y está compuesto por cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue (4) .

Este modelo representa un salto cualitativo en el paradigma computacional actual. De la infraestructura y las aplicaciones dominadas y administradas por las propias organizaciones, se pasa a otro donde un tercero, en principio confiable y conocido, brinda capacidad de infraestructura, plataformas o servicios de software.

Asimismo, el modelo de servicios de cómputo en la nube presenta tres alternativas distintas: Infrastructure as a Service (IaaS), Plataform as a Service (PaaS) y Software as a Service (SaaS).

Los servicios de Cloud Computing son uno de los principales facilitadores de Big Data. Mucha de la información recolectada por los dispositivos antes mencionados será almacenada por proveedores de servicios de Cloud Computing. Es en estos servicios que esos datos serán procesados y analizados, otorgando grandes beneficios como el acceso desde cualquier parte del mundo, la flexibilidad y escalabilidad de los recursos y la posibilidad de auto gestionar a distancia los recursos informáticos. Así, Cloud Computing (principalmente los modelos PaaS y IaaS) brindarán la infraestructura básica para el procesamiento de datos necesario en el análisis de grandes volúmenes de información.

Sin embargo, el uso de servicios de cómputo en la nube genera riesgos específicos, tanto en términos de privacidad como de seguridad de la información. Los riesgos están vinculados de forma directa con la localización de los datos, la falta de información sobre las condiciones en la que se presta el servicio, la falta de control del responsable sobre el uso y gestión de los datos personales por parte de los implicados en el servicio y la jurisdicción donde se encuentran localizados los datos.

Son estos factores los que adicionan un mayor esfuerzo (tanto de índole técnico como organizacional) para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida o consulta no autorizada, y que permiten detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

IV. Riesgos de la actividad

Por otro lado, este fenómeno tecnológico, de amplia aplicación al día de la fecha, pone en riesgo en forma directa el derecho a la protección de los datos personales, la privacidad de los individuos y el libre desarrollo de su personalidad.

Es innegable el impacto negativo que tiene en la privacidad de las personas el hecho de que sus datos puedan ser recogidos sin que se percaten de ello, para la posterior generación de múltiples flujos de información para la intervención de una pluralidad de actores, que puede permitir que los datos acaben siendo destinados a usos muy distintos de los originalmente previstos, como por ejemplo la formación de perfiles.

Asimismo, la aplicación de perfiles a las personas puede ocasionar serias repercusiones, no solo en su privacidad, sino en una multiplicidad de sus derechos, que pueden verse eventualmente afectados por decisiones de terceros tomadas con base en tales perfiles.

En tal sentido, la actividad de Big Data genera nuevos datos personales que, en muchos casos, son utilizados para enriquecer perfiles para su posterior asignación a un individuo determinado. Por ejemplo, en algunos casos, al incluir a una persona en un perfil perteneciente a un grupo social previamente analizado con esta tecnología, se puede estimar su nivel de ingresos o, sobre la base de su edad, una posible afectación de su salud.

Existen nuevas formas de recolección de datos personales, como ya dijimos, a través de dispositivos conectados a Internet -Internet de las Cosas-, pero aún más novedosa es la posibilidad de tomar información personal a través de satélites de observación de la tierra (5). Estos satélites cuentan con la capacidad de tomar fotografías a personas desde 600 kilómetros de altura, con una resolución menor a 30 cm. Con estas capacidades en el campo de la observación de la tierra (sobre todo de capacidades de monitoreo en alta resolución), combinadas con grandes volúmenes de información provenientes de Internet, el contexto actual brinda a los usuarios de estos servicios grandes beneficios a bajo costo: acceso a información en tiempo real para la toma de decisiones diarias en industria, gobierno, gestión de recursos naturales, generación y distribución de energía y producción de alimentos, como así también información de geolocalización personalizada. Pero, a su vez, tienen la capacidad de generar importantes riesgos a la privacidad de las personas.

Esta asignación de determinadas características a las personas por su supuesta pertenencia un perfil específico se presenta como una hipótesis -y ha de ser tratada como tal- y, por lo tanto, no debe ser utilizada para la toma de decisiones que puedan afectar los derechos de los individuos. Y siempre, en toda circunstancia, debe ser informada al titular del dato para que pueda, de ser necesario, realizar las acciones que considere tener derecho para la mejor protección de sus intereses.

V. La aplicación de la ley 25.326 a las actividades de Big Data

La ley 25.326 tiene como objetivo proteger los datos personales asentados en archivos, registros, bancos de

datos u otros mecanismos técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes, otorgando protección a las personas sobre sus derechos al honor e intimidad y acceso a la información personal, de conformidad con lo establecido en el art. 43, párrafo tercero, de la Constitución Nacional.

A tal fin, la ley 25.326 reglamentó la actividad de quienes realizan tratamientos de datos personales, como los archivos o bancos de datos que procesan información personal por medios técnicos, sean informáticos o manuales, y los sometió al control de la Dirección Nacional de Protección de Datos Personales (PDP) en el ámbito nacional (art. 29 y 44 de la ley 25.326). Las disposiciones de los Capítulos I, II, III, IV y el art. 32 de la ley 25.326 son de orden público, conforme lo dispone el art. 44 de la misma normativa.

Según cuáles sean las actividades de tratamiento, la ley previó distintas condiciones de licitud, que se clasifican en requisitos y principios. Serán requisitos cuando se requieran actos o medidas determinadas por parte del responsable del tratamiento (condicionamientos concretos), y serán principios cuando consistan en pautas de calidad del tratamiento (directrices de conducta).

Para la interpretación adecuada de estas condiciones de licitud, debe tenerse en cuenta que estas no pueden afectar otros intereses y derechos, sino consistir en una adecuada armonización de ellos (6) y, por otro lado, que no pueden llevar a resultados paralizantes de la actividad informativa (7).

Hay dos momentos de particular sensibilidad en el tratamiento de datos personales: cuando se recolectan y cuando se transfieren a terceros mediante cesión, transferencia internacional o prestación de servicios; casos especialmente regulados por la ley 25.326.

La ley 25.326 dispuso dos requisitos básicos que son condición de licitud de todo tratamiento: a) requerir el consentimiento previo del titular del dato (art. 5º) (8); y b) brindar información sobre el tratamiento previsto al titular del dato (art. 6º) (9).

Tiene particular relevancia en el presente caso de Big Data el principio de finalidad, que dispone que "los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención". Sobre esa base, cuando los datos pretendan ser utilizados para otra finalidad, requerirán el consentimiento previo del titular del dato.

a) Requisito del consentimiento previo - Finalidad

El artículo 5º de la ley 25.326 expresamente dispone que "el tratamiento de datos personales será ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado", estableciendo varias excepciones. Resulta relevante en el presente análisis, la prevista con vistas al caso en que los datos sean necesarios para el desarrollo de una relación contractual (cabe entender, aquella en la que el titular del dato sea parte).

En tal sentido, en las actividades de Big Data realizadas por las empresas para brindarle un mejor servicio al titular del dato, no sería necesario el consentimiento, en la medida que no se extralimite de tales fines contractuales.

En sentido contrario, será necesario el consentimiento previo e informado del titular del dato para el desarrollo de análisis de Big Data sobre datos personales en los que la finalidad del tratamiento sea distinta o no compatible con la que motivó su recolección, salvo que sean datos disociados (cfr. art. 28 de la ley 25.326) (10).

b) Deber de informar

Es un requisito esencial para la licitud de todo tratamiento de datos personales el informar a quienes vayan a ser objeto de tratamiento, con la amplitud y detalle necesarios, respecto de las características y finalidades del tratamiento, en particular: a) la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) la existencia del banco de datos, identidad y domicilio de su responsable; c) el carácter obligatorio o facultativo para brindar los datos requeridos; d) las consecuencias; e) la posibilidad del titular del dato de ejercer sus derechos de acceso, rectificación y supresión (cfr. art. 6 ley 25.326 referenciado supra) (11).

Este requisito tiene particular relevancia en las actividades de Big Data, exigible tanto respecto de la utilización de datos personales en las actividades de análisis, como también respecto de la asignación a las personas de datos y/o perfiles obtenidos mediante dichas técnicas. En efecto, conforme a lo dispuesto por el art. 6º de la ley 25.326, el responsable del tratamiento debe informar en todo momento al titular del dato sobre la modalidad de utilización de sus datos, requisito que toma aún más fuerza en estas circunstancias en las que el tratamiento se aboca al análisis y estudio de conductas y eventual combinación con datos obtenidos de terceros, o incluirlo en determinados perfiles, pues el titular del dato debe saber los riesgos a los que se enfrenta su información personal y eventual afectación de sus derechos o intereses, a fin de que pueda ejercitar en plenitud todos sus derechos.

En tal sentido, conforme lo expuesto supra en punto anterior, no obstante que será lícito, en el marco de una relación contractual, tratar datos personales para la elaboración de perfiles sin el consentimiento del titular del dato, no se exceptúa de manera alguna el deber de informar al titular del dato.

Este deber de informar subsiste aun cuando los datos vayan a ser utilizados anónimamente, a fin de que el titular del dato sepa todas las finalidades a las que se destinarán sus datos, aun frente a riesgos hipotéticos.

VI. Calidad del dato

Como se señaló, la ley 25.326 establece que para la licitud de todo tratamiento se debe requerir el consentimiento previo del titular del dato y también brindar información sobre el tratamiento previsto a su titular. Estos requisitos básicos se complementan con los principios dispuestos por el art. 4º de la ley 25.326, aplicables a todo tratamiento de datos personales.

A fin de determinar la calidad de los datos, se deben tener en cuenta los siguientes parámetros de evaluación:

a) Información confidencial: es aquella afectada por un secreto o confidencialidad legal (ej. secreto profesional, bancario, fiscal, datos sensibles, etc.), derechos de terceros (ej. intimidad), entre otros. Para el presente caso, debe analizarse si la información a solicitar ha sido declarada confidencial por alguna ley, y si esta habilita el tratamiento a ambos organismos; extremo que puede ser determinado por las partes contratantes. También debe analizarse si los datos a tratar se califican como dato sensible, definidos como prohibidos por la ley 25.326 en su art. 2, que declara, en protección de la intimidad de las personas, como sensibles a los siguientes datos: origen racial, étnico, opiniones políticas, religiosas, filosóficas, morales, afiliación sindical, referidos a la salud y vida sexual. En tal sentido, se entiende que la ley 25.326 ha dejado en claro una larga discusión doctrinaria y jurisprudencial: la determinación de cuáles son los datos íntimos y, por tanto, prohibidos para su tratamiento por parte de terceros. Al respecto, el art. 7° de la ley 25.326 expresamente dispone:

1. Ninguna persona puede ser obligada a proporcionar datos sensibles (aquellos que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual).

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas asi como las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes en el marco de las leyes y reglamentaciones respectivas.

Sobre la base de la normativa transcripta, los datos sensibles no podrían intercambiarse si ambos organismos no se encuentran autorizados por ley para su tratamiento.

b) Información pública: es la información en poder de la Administración que no está sujeta a confidencialidad ni tampoco está destinada a ser difundida irrestrictamente al público, y que generalmente su acceso por parte de terceros resulta condicionado al cumplimiento de ciertos requisitos. En esta categoría no encontramos impedimento alguno para su cesión, salvo el cumplimiento del requisito de la competencia. Al respecto, cabe destacar el reciente decreto 1172/03, Anexo VII, especialmente los arts. 8, 11, 12 y 16.

c) Información pública irrestricta: es aquella información destinada a ser difundida al público en general y de libre intercambio entre los Organismos del Estado. Esta clasificación en tres niveles de intensidad de la publicidad de los datos a tratar (información confidencial, pública y pública irrestricta) permite a las partes concluir si los datos a ceder cumplen con los requisitos de ley y, más específicamente, que no contienen información prohibida (ej. datos sensibles o información declarada secreta por ley). Por los motivos expuestos, las partes deberían contemplar estos conceptos e incluirlos en una eventual cláusula específica de análisis de la calidad y/o categoría del dato a tratar ("naturaleza y calidad del dato a tratar por las partes"), detallando las categorías de datos a contratar y concluyendo sobre la legitimidad de su tratamiento, sobre lo arriba expuesto.

VII. Disociación de datos

En muchas ocasiones, la generación de perfiles a partir de análisis de grandes volúmenes de datos no supone un tratamiento con efecto sobre el titular del dato, al tratarse disociados y/o utilizados para la elaboración de un patrón de comportamiento social, sin referirlos a personas determinadas. En tal caso, el titular del dato no sufre ningún ataque a su privacidad, y la entidad que explota los datos puede generar un valor a partir de los perfiles

creados, proporcionando, por ejemplo, un servicio a otros individuos que sí consientan que sus datos sean comparados con los patrones definidos.

En caso de utilizar datos personales que sean disociados para afectarlos al servicio de Big Data, el responsable deberá: a) tomar las medidas necesarias para que no sea razonablemente posible una posterior determinación de su titular y, b) informar previamente a los titulares de los datos de dicho tratamiento.

VIII. No automaticidad

En caso de que la aplicación de dicho perfil en una operación determinada genere algún perjuicio a los derechos o intereses del titular del dato, como lo sería por ejemplo en el caso de una negativa a una solicitud de préstamo, además de informársele sobre tal hecho (cfr. art. 6º ley 25.326 y art. 1387 del Código Civil y Comercial de la Nación) (12), se deben establecer mecanismos para anteponer a dicha decisión una revisión no automatizada, esto es, brindar una alternativa distinta a la automatizada que garantice un juicio de valor específico para su situación personal o un eventual descargo.

En caso de no brindarse un mecanismo o alternativa adecuada a las circunstancias del caso, el titular del dato podrá plantear la ilicitud del tratamiento en tales condiciones (cfr. art. 1717 del Código Civil y Comercial de la Nación (13)).

IX. Derecho de oposición

Además del requisito del consentimiento previo, el derecho a la protección de datos personales, en virtud de las facultades de autodeterminación y disposición, otorga al titular del dato el derecho a oponerse a un tratamiento que, por razones particulares, le genere un perjuicio, por lo que en dichos casos ha de reconocerse el derecho de las personas a oponerse a la elaboración o asignación de perfiles.

X. Recomendaciones para un tratamiento seguro

Algunos tratamientos de datos personales más riesgosos requieren medidas específicas para garantizar un tratamiento seguro. En tal sentido, dado el riesgo que la actividad de Big Data implica para los titulares de los datos y sus derechos, se requieren medidas específicas para su tutela (14), por lo que se recomienda que, previamente y durante dicho tratamiento, el responsable tome al menos las medidas que se indican a continuación (15):

a) Estudio de impacto de privacidad . Antes de la realización de tareas de Big Data sobre datos personales, el responsable deberá efectuar un estudio de impacto sobre la privacidad de sus titulares, a fin de determinar los riesgos actuales y potenciales en la privacidad y derechos de las personas (ej. perfiles y predicción de conductas que puedan obtenerse con dicho tratamiento).

b) Política de privacidad. El responsable deberá elaborar una política de privacidad que incorpore en su texto las medidas de protección de datos personales dispuestas por la empresa y que contenga las siguientes condiciones: a) cumplimiento de los principios y requisitos de licitud dispuestos por la ley 25.326, indicando las medidas dispuestas; b) se indique las finalidades del tratamiento previsto; c) se haga saber si utiliza o no la disociación en su tratamiento y se indique la modalidad implementada; d) la información que brindará al titular del dato para el conocimiento del tratamiento, con especial detalle si el tratamiento pudiera eventualmente afectarlo en alguno de sus derechos; e) los casos en que prevea requerir el consentimiento del titular del dato; f) el modo de recolección de los datos objeto de tratamiento (con consentimiento previo, o con motivo del cumplimiento de un contrato, en forma subrepticia u ostensible, etc.); g) forma en que se enriquecen los datos -incorporación del valor agregado- (ej. sobre datos anónimos o sobre datos identificados y luego disociados); h) análisis y técnicas a los que se prevé someter los datos (ej. generación de perfiles, enriquecimiento con fuentes de terceros, Data Mining, Machine Learning, Social Network Analysis, Predictive Analytics, Sensemaking, Natural Language Processing and Visualization, etc.); i) condiciones para determinar la caducidad del dato, según la finalidad que justificó originalmente su recolección (finalidad principal) (el Big Data no puede ser causal de conservación sin plazo, pues siempre serán útiles, salvo que se anonimicen o se consienta específicamente esa característica); j) medidas para el respeto de los principios de calidad del dato y por las que se garanticen que solo se utilizarán datos que sean estrictamente necesarios y no excesivos para la finalidad prevista; k) medidas dispuestas para el cumplimiento de los derechos del titular del dato, en caso de que no se utilicen datos disociados (acceso, rectificación, oposición y supresión); l) las medidas de "privacy by design" que se prevean incorporar, en razón del resultado que determine el estudio de impacto de privacidad; m) las medidas de seguridad y confidencialidad dispuestas, de acuerdo a las características del tratamiento (art. 9 y 10 de la ley 25.326 y disposición DNPDP Nº 11/2006).

c) Compromiso respecto de las condiciones de licitud particularmente aplicables: 1) no utilizará los datos personales para fines distintos o incompatibles a los que se denunciaron al momento de su recolección, 2) no

implicará un uso del dato personal más allá de lo estrictamente necesario para la finalidad de su recolección, 3) se informará al titular del dato en forma totalmente transparente respecto de los tratamientos previstos y sus consecuencias, aun las eventuales, 4) no realizará tratamiento de datos sensibles, tanto en su recolección como en los análisis previstos (se eliminarán en caso de detectar tal consecuencia con motivo de los análisis efectuados), 5) en caso de disociar los datos se tomarán todas las medidas necesarias para que no sea razonablemente posible una posterior determinación de su titular, 6) no se utilizarán las conclusiones de análisis de tratamiento que no sean seguras cuando puedan afectar un derecho o interés relevante del titular del dato, 7) ha determinado que las finalidades del análisis previsto no resultan contrarias a la ley, moral y buenas costumbres, el principio de buena fe y normas del arte, y en particular que no se utilizará para obtener un mayor control o manejo de la voluntad de las personas, velando en toda instancia por el libre desarrollo de su personalidad y el respeto de todos sus derechos; 8) que no se utilizará el tratamiento y su análisis como parte determinante en la toma de decisiones que afecten derechos de las personas, 9) no se realizarán análisis que produzcan discriminación o exclusión social, y/o afecten el pleno desarrollo de la personalidad de las personas, 10) en caso de adquisición de datos de terceros, tomará los recaudos necesarios según el caso para verificar su legalidad (informe de auditoría, dictamen previo, etc.), 11) tanto al estudio de impacto de privacidad como la política de privacidad arriba indicadas serán ampliamente difundidas por el responsable para su conocimiento por el titular del dato, a fin de que pueda determinar en qué puede beneficiarlo y/o afectarlo, favoreciendo así el otorgamiento de facultades al usuario para la protección de sus derechos (esta información deberá brindarse al titular del dato aun cuando se trabaje sobre sus datos disociados); 12) en caso de transferirse los datos a terceros países, y estos no tengan legislación adecuada, deberá cumplirse con los requisitos del art. 12 de la ley 25.326 y el Anexo I del decreto 1558/2001; 13) en caso de prestación de servicios de Big Data por parte de terceros, deberá darse cumplimiento a lo dispuesto por el art. 25 de la ley 25.326 y el Anexo I del decreto 1558/2001.

XI. Conclusiones

Como se expuso en este artículo, la capacidad de almacenar y analizar grandes cantidades de datos puede generar innumerables beneficios para la sociedad. Sin embargo, también puede vulnerar de forma significativa la privacidad de las personas y su derecho a la auto determinación informativa.

Esta nueva forma de procesar la información puede asociarse a su capacidad para hacer predicciones acerca de acciones, comportamientos o eventos futuros. Es por ello que debemos entender que la protección de principios como los de limitación de la finalidad y la minimización de datos son fundamentales para garantizar la privacidad de las personas, sobre todo en contextos donde se recopila una cantidad cada vez mayor de información sobre nosotros.

A su vez, un factor que aportará transparencia y seguridad a las empresas dedicadas al tratamiento masivo de datos personales es la aplicación de los principios de la privacidad desde el diseño (16), los cuales promueven que el titular de los datos de carácter personal mantenga mayor control sobre sus datos, el tratamiento que se les da y las medidas de seguridad que se les aplican.

El debilitamiento de los principios clave de privacidad, junto con un mayor uso del Big Data, es probable que tengan consecuencias adversas para la protección de la privacidad y de otros derechos fundamentales. Por ello, los proveedores de estos servicios deberán estar atentos a respetar el principio de especificación de finalidad; limitar la cantidad de información recolectada y almacenada a un nivel que sea necesario para el propósito legítimo que pretende; solicitar el consentimiento del titular de los datos en relación con el uso de información personal para fines de análisis y de creación de perfiles y, si la información recolectada es transferida a terceros, deberá informarse de forma adecuada al titular del dato.

(1) SEGURA, P. (2014) "Internet de las Cosas". En Travieso, J. A. (Director) "Régimen jurídico de los datos personales", t. I. Buenos Aires: Editorial La Ley, (pp. 521-537).

(2) EVANS, D. (2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything". Disponible al 14/12/15 http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

(3) Stamford, C. (2015) Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities. Gartner Press Release. Disponible al 25/12/15 http://www.gartner.com/newsroom/id/2970017

(4) Mell P., Grance T., (2011) "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-145.

(5) GONZÁLEZ ALLONCA, Juan Cruz. "El tratamiento de los datos personales y la teleobservación de la Tierra desde el espacio". L.L. Sup. Act. 07/10/2014, 1.

(6) Las restricciones de los derechos no podrán realizarse afectando su contenido esencial. Al respecto, ver TOLLER, Fernando, "Los derechos in concert. Metodologías para tomar decisiones armonizadoras en casos entre derechos y bienes constitucionales", en Juan Cianciardo (Coord.), Constitución, Neoconstitucionalismo y Derechos. Porrúa: México, 2012, 136: "Siempre que pueda establecerse que existe una limitación o restricción legal o jurisprudencial a un derecho, que implicará naturalmente que se lo recorta o altera, ese tratamiento será inconstitucional. Quien regula actúa constitucionalmente, pero quien restringe o limita en verdad altera, viola el contenido esencial, infringe la propia Constitución. Por ello, no es posible las intromisiones legítimas en el ámbito de funcionamiento razonable de un derecho...".

(7) Resulta muy ilustrativo trascribir aquí la opinión de Grupo de Trabajo del art. 29, Directiva 95/46/CE, a través de su Dictamen 4/2007 sobre el concepto de datos personales:"Aparte de las exenciones que tienen su origen en el ámbito de aplicación del Derecho comunitario, las exenciones previstas en el art. 3 de la Directiva tienen en cuenta la forma técnica del tratamiento (en forma manual no estructurada) y el fin con el que se utilizan (para las actividades exclusivamente personales o domésticas efectuadas por una persona física). Pero, incluso en el supuesto de que el tratamiento de datos personales entre en el ámbito de la Directiva, puede que no todas sus normas sean aplicables al caso concreto. Varias disposiciones de la Directiva tienen un grado de flexibilidad considerable, con el fin de lograr un equilibrio adecuado entre la protección de los derechos del interesado, por un lado, y los posibles intereses legítimos de los responsables del tratamiento de datos, las terceras personas y el interés público, por otro (...) En aquellos casos en que, a primera vista, una aplicación mecánica de una determinada disposición de la Directiva provoque una carga excesiva o incluso consecuencias absurdas, deberá comprobarse previamente: 1) si la situación entra en el ámbito de aplicación de la Directiva, en particular con arreglo a su art. 3; y 2) cuando así sea, si la propia Directiva, o la legislación nacional adoptada de conformidad con ella, no admite exenciones o simplificaciones en situaciones particulares con el fin de lograr una respuesta legal apropiada, asegurando al mismo tiempo la protección de los derechos de la persona y los intereses en juego. La mejor opción es no restringir indebidamente la interpretación de la definición de datos personales, sino tener en cuenta que existe una considerable flexibilidad en la aplicación de las normas a los datos. Las autoridades nacionales encargadas de supervisar la protección de datos tienen un rol esencial a este respecto dentro de su función de supervisión de la aplicación de la legislación sobre protección de datos, que conlleva interpretar las disposiciones legales y proporcionar orientación concreta a los responsables y los interesados. Esas autoridades deberían aprobar una definición lo suficientemente amplia para anticiparse a las posibles evoluciones y cubrir todas las «zonas grises» existentes en su ámbito de aplicación, haciendo al mismo tiempo uso legítimo de la flexibilidad que caracteriza a la Directiva. De hecho, el texto de la Directiva invita a elaborar una política que combine una interpretación lata del concepto de datos personales y un equilibrio apropiado en la aplicación de sus normas".

(8) Ley 25.326:"Articulo 5° — (Consentimiento). 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526".

(9) Ley 25.326:"Articulo 6° — (Información). Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos".

(10) Ver el documento de trabajo del grupo International Working Group on Data Protection in Telecommunications, "Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics", 55th Meeting, 5 — 6 May 2014, Skopje. Disponible al 31/08/15 en http://www.privacy.mk/

en/node/2736.

(11) Anexo I del Decreto 1558/2001:"Articulo 5º.- El consentimiento informado es el que está precedido de una explicación, al titular de los datos, en forma adecuada a su nivel social y cultural, de la información a que se refiere el artículo 6º de la Ley Nº 25.326...".

(12) Ver al respecto lo dispuesto por el nuevo Código Civil y Comercial de la Nación sobre relaciones de consumo:"Articulo 1387.- Obligaciones precontractuales. Antes de vincular contractualmente al consumidor, el banco debe proveer información suficiente para que el cliente pueda confrontar las distintas ofertas de crédito existentes en el sistema, publicadas por el Banco Central de la República Argentina. Si el banco rechaza una solicitud de crédito por la información negativa registrada en una base de datos, debe informar al consumidor en forma inmediata y gratuita el resultado de la consulta y la fuente de donde la obtuvo".

(13) Código Civil y Comercial de la Nación:"Articulo 1717.- Antijuridicidad. Cualquier acción u omisión que causa un daño a otro es antijurídica si no está justificada"."Articulo 1716.- Deber de reparar. La violación del deber de no dañar a otro, o el incumplimiento de una obligación, da lugar a la reparación del daño causado, conforme con las disposiciones de este Código".El anterior Código Civil disponía con claridad, en su art. 1109: "Todo el que ejecuta un hecho, que por su culpa o negligencia ocasiona un daño a otro, está obligado a la reparación del perjuicio...". El nuevo Código genera cierta confusión sobre la aplicación de este principio en los artículos art. 1717 y 1718 que eximen dicha responsabilidad en caso de ejercicio de un derecho, cuestión que requerirá una correcta interpretación para no vaciar su contenido esencial.

(14) Ver documento del Grupo de Trabajo del art. 29 de la Directiva 65/46/CE [Article 29 Working Party (WP29)] "Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU" (disponible al 31/8/15 en el sitio http://ec.europa.eu/justice/data-protection/index_en.htm).

(15) Ver al respecto lo desarrollado por el Comisionado de la Información del Reino Unido (Information Commissioner´s Office, ICO), a través del documento "Big data and data protection", 20140728, Version: 1.0 (disponible al 31/8/15 en Internet en la dirección https://ico.org.uk/media/1541/big-data-and-data-protection.pdf).

(16) Cavoukian, A. (2009) Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.