Buenas Prácticas para la Protección de Datos Personales en ambientes de Big Data

Juan C González Allonca[1], Esteban Ruiz Martínez [2], Ma Florencia Pollo-Cattaneo [1]

[1] Grupo de Estudio en Metodologías de Ingeniería de Software (GEMIS). Facultad Regional Buenos Aires. Universidad Tecnológica Nacional, Ciudad Autónoma de Buenos Aires, Argentina
{juanallonca,flo.pollo} @gmail.com

[2] Asesor de la Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia y Derechos Humanos de la Nación, Sarmiento 1118 (C1041AAX), Ciudad Autónoma de Buenos Aires, Argentina
estebanruizmartinez@gmail.com

Resumen. El modelo de procesamiento de grandes volúmenes de datos o Big Data ofrece múltiples ventajas, tanto técnicas como económicas para las empresas y organismos que deciden implementarlo. Este modelo, sin embargo, requiere tener consideraciones de carácter legal y de cumplimiento normativo desde el inicio del proyecto. El presente estudio se propone recorrer la normativa argentina relativa a la protección de datos personales y su relación con este modelo de cómputo, brindando un panorama sobre el cuerpo normativo vigente que debe ser aplicado a servicios de Big Data. A su vez, identifica los riesgos asociados a estos servicios que deben ser contemplados, con el fin de evitar responsabilidades. Asimismo, analizará la actividad de Big Data en el contexto de Internet de las Cosas y Cloud Computing.

1 Introducción

En los últimos tiempos, los avances en las Tecnologías de la Información y la Comunicación (TIC) permiten generar, transmitir y almacenar grandes cantidades de información [1-2]. Los conjuntos de datos son tan grandes y complejos, y se generan tan rápido, que los enfoques tradicionales del procesamiento de información son insuficientes e inadecuados. Proponer un análisis eficiente de los datos dentro de plazos aceptables supone un desafío, al que la industria responde utilizando tecnologías en el campo de Big Data [3-4-5-6].

Los sistemas de información, a través de sus aplicaciones de tratamiento de datos personales, pueden fácilmente invadir ámbitos reservados de la persona que, hasta hace poco, eran inaccesibles, como, por ejemplo, su intimidad [7]. En este contexto es necesario determinar un equilibrio entre dos conceptos 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 mayor 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 [8]. 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, 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 del modelo computacional conocido como Big Data, que tiene por objeto el análisis de grandes cantidades de datos, estructurados o no [9]. Esta tecnología realiza el tratamiento de datos con complejos algoritmos que permiten obtener nueva información sobre las personas y que, muchos anticipan, se convertirá en una herramienta clave del desarrollo, impulsando nuevas olas de crecimiento en la productividad en los modelos de negocios que las utilizan [10].

Interesa en este trabajo identificar las características jurídicas más relevantes del modelo de Big Data vinculadas a los derechos de la persona, en particular, el derecho a la intimidad y la protección de los datos personales y, a su vez, proponer pautas de licitud para su uso en la Argentina.

Para ello, en este artículo primero se describen las características principales de la asignatura considerada (Sección 2) y de la tecnología aplicada (Sección 3). Luego, se presentan los riesgos de la actividad (Sección 4), la aplicación de la ley de protección de datos personales (Sección 5), y recomendaciones para un tratamiento seguro (Sección 6). Finalmente, se indican las conclusiones del trabajo y futuras líneas de trabajo (Sección 7).

2 Características del Big Data

Son características definitorias del paradigma de Big Data el tratar información en grandes volúmenes [11], 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.

A través de la publicación de la Recomendación UIT-T Y.3600 "Grandes volúmenes de datos – requisitos y capacidades basados en la computación en la nube"[12], la Unión Internacional de Telecomunicaciones (UIT), ha aprobado la primera norma sobre los grandes volúmenes de datos o Big Data. Además de la descripción de los fundamentos de Big Data basados en la nube, la UIT-T Y.3600 facilita las definiciones de

Big Data y los Big Data como Servicio (BDaaS). Por un lado, la de Big Data, la cual define como paradigma para hacer posible la recopilación, el almacenamiento, la gestión, el análisis y la visualización, potencialmente en condiciones de tiempo real, de grandes conjuntos de datos con características heterogéneas.

Por otro lado, identifica a Big Data como Servicio (BDaaS) como una categoría de servicio en la nube en la que las capacidades que se ponen a disposición del cliente del servicio en la nube le permiten recopilar, almacenar, analizar y visualizar los datos utilizando tecnologías Big Data.

Resulta de interés para este análisis que 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, datos de geolocalización, entre otras.- 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, entre otros), y determinar así la toma de decisiones por parte de los actores económicos del mercado [13]. 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 hubieran 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.

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

El impulso de Big Data trae aparejados beneficios económicos y sociales y, a su vez, genera un desafío en términos de privacidad y protección de datos personales [14-15]. Su desarrollo se da en un contexto marcado por rápidos avances tecnológicos, de los cuales se destacan por su alcance y por la complementariedad que los une con Big Data: Internet de las Cosas o Internet of Things (IoT) y los servicios de Cloud Computing [16].

Internet de las Cosas es un concepto que se refiere a la conexión de objetos cotidianos a Internet. Como Señala Segura [17],

> 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.

Según un estudio realizado por la empresa de equipos de telecomunicaciones *Cisco Systems* [18], en 2012 había 8.700 millones de objetos conectados a Internet; en la

actualidad esta cifra alcanza los 25.000 millones y, en 2020, se esperan más de 50.000 millones, es decir, 6,58 dispositivos conectados a Internet por cada habitante de la Tierra. 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 integran la IoT es innumerable y abarca múltiples ámbitos:

1) 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 [19].

2) W*earable computing*: es la integración entre los dispositivos y la vestimenta o accesorios, para medir signos vitales [20] (prendas capaces de monitorear las condiciones climáticas y las preferencias del usuario, adaptándose al ambiente).

3) Los automóviles conectados también harán uso de IoT, a través de la conducción automatizada y servicios a bordo. Según un estudio de *Gartner*, para el año 2020 circularán en el mundo más de 250 millones de autos conectados a Internet [21].

4) S*mart cities*, que implican 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 [22], 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 [23-24].

Por último, se considera otra variable tecnológica clave que se conjuga 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 [24].

Esta propuesta tecnológica 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) [25].

Los servicios de Cloud Computing se constituyen como 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 [26]. 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.

4 Riesgos de la Actividad

El fenómeno tecnológico de Big Data, 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 [27-28-29-30]. Un ejemplo que ilustra los riesgos que puede traer aparejado el uso de Big Data es el llamado “Algoritmo del embarazo” [31]. Como evidencia este ejemplo, es claro el impacto negativo que puede tener 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 en base a 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, en base a su edad, una posible afectación de su salud [32-33-34].

La 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. 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.

5 La aplicación de la ley 25.326 a las actividades de Big Data[1]

La ley N° 25.326 de protección de datos personales [35] tiene como objetivo proteger la información personal asentada 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 reglamenta 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 somete 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[2], conforme lo dispone el art. 44 de la misma normativa.

Según cuáles sean las actividades de tratamiento, la ley prevé 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) [35].

[1] Para este trabajo se entiende por “aplicaciones de Big Data” y “servicios de Big Data” a aquellas aplicaciones y servicios que para su realización implican el tratamiento de datos personales.

[2] Como señala Guillermo Borda en su Tratado de Derecho Civil Parte General, “las leyes de orden público son leyes imperativas”, es decir, responden a un interés general, colectivo, es decir fundamental para regular el orden social del país, por oposición a las cuestiones de orden privado, en las que sólo juega un interés particular. Por ello las leyes de orden público son irrenunciables (BORDA, Guillermo. Manual de Derecho Civil: parte general. 13. ed. Buenos Aires: Perrot, 1986, p. 44).

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

Existen dos momentos de particular sensibilidad en el tratamiento de datos personales: cuando se recolectan y cuando se transfieren a terceros, sea mediante cesión, transferencia internacional o prestación de servicios; y, por tales motivos, todos ellos son casos especialmente regulados por la ley 25.326. Asimismo, esta ley dispuso dos requisitos básicos que son condición de licitud de todo tratamiento: a) requerir el consentimiento previo del titular del dato (art. 5º), y b) brindar información al titular del dato (art. 6º). Tiene particular relevancia en el presente caso de Big Data el principio de finalidad, sobre el que la ley 25.326 dispone: "los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención". En base al mismo, cuando los datos pretendan ser utilizados para otra finalidad, requerirán el consentimiento previo del titular del dato.

5.1 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 para el presente análisis, la prevista para el 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.

Sin embargo, 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).

5.2 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).

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 Nº 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 anteriormente, 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.

5.4. Calidad del Dato

El principio de calidad del dato, establecido en el artículo 4º de la ley 25.326 exige que los datos sean ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. A su vez, el mismo artículo señala que para la licitud de todo tratamiento de información personal se debe requerir el consentimiento previo del titular del dato y también brindar información sobre el tratamiento que se le hará a los mismos. Por ello, se debe analizar si los datos a tratar son adecuados para la finalidad prevista, y en especial si la categoría de los mismos lo califican como dato sensible, definidos como prohibidos por la ley 25.326 en su art. 2 (origen racial, étnico, opiniones políticas, religiosas, filosóficas, morales, afiliación sindical, referidos a la salud y vida sexual) que en base al artículo 7 de la ley citado su tratamiento se encuentra prohibido salvo que estuviese previsto por ley fundada en razones de interés general.

La adecuación del dato no solo se encuentra definida por ser una categoría legalmente admisible, sino también cuando es cierto, pertinente, no excesivo, completo y actualizado para la finalidad del tratamiento previsto (*cfr*. art. 4º de la ley 25.326).

5.5. 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 [36-37]. En tal caso, el titular del dato no sufre

ninguna vulneración 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 debe: a) tomar las medidas necesarias para que no sea razonablemente posible una posterior determinación de su titular y, b) aun en tal caso, informar previamente a los titulares de los datos de dicho tratamiento.

5.6. 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 tal hecho (*cfr*. art. 6º ley 25.326 y art. 1387 del Código Civil y Comercial de la Nación), 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).

5.7. 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. Esto es procedente cuando lo requieran los principios y/o requisitos de licitud que establece la ley (arts. 16 y 33 de la ley 25.326).

6. 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, por lo que se recomienda que, previo y durante dicho tratamiento, el responsable tome al menos las medidas basadas en la Ley 25.326 y los principios de protección de datos personales que se indican a continuación:

a) Estudio de impacto de privacidad: previo a la realización de tareas de Big Data sobre datos personales, el responsable debe 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 debe 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:

1) cumplimiento de los principios y requisitos de licitud dispuestos por la ley 25.326, indicando las medidas dispuestas;

2) indique las finalidades del tratamiento previsto;

3) haga saber si utiliza, o no, la disociación en su tratamiento, e indique la modalidad implementada;

4) otorgue información detallada al titular del dato sobre su tratamiento, especialmente si el tratamiento pudiera eventualmente afectarlo en alguno de sus derechos;

5) los casos en que prevea requerir el consentimiento del titular del dato;

6) 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);

7) forma en que se enriquecen los datos - incorporación del valor agregado- (ej. sobre datos anónimos o sobre datos identificados y luego disociados);

8) análisis y técnicas a las 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);

9) condiciones para determinar la caducidad del dato, según la finalidad que justificó originalmente su recolección (finalidad principal). Big Data no puede ser causal de conservación sin plazo, pues siempre serán útiles, salvo que se anonimicen o se consienta específicamente esa característica;

10) 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;

11) 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);

12) las medidas de "privacidad desde el diseño" que se prevean incorporar, en razón del resultado que determine el estudio de impacto de privacidad;

13) las medidas de seguridad y confidencialidad dispuestas, acordes a las características del tratamiento (art. 9 y 10 de la ley 25.326 y Disposición DNPDP Nº 11/2006).

c) Condiciones específicas de licitud: garantizar las condiciones de licitud para el tratamiento de datos personales aplicables a ambientes de Big Data.

1) no utilizar los datos personales para fines distintos o incompatibles a los que se denunciaron al momento de su recolección;

2) no involucrar el uso de datos personales más allá de lo estrictamente necesario para la finalidad de su recolección;

3) informar al titular del dato de manera totalmente transparente respecto de los tratamientos previstos y sus consecuencias, aun las eventuales;

4) no realizar 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, tomar todas las medidas necesarias para que no sea razonablemente posible una posterior determinación de su titular;

6) no utilizar las conclusiones de análisis de tratamiento que no sean seguras cuando puedan afectar un derecho o interés relevante del titular del dato;

7) determinar 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 utiliza a fin de 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) no se utilizar el tratamiento y su análisis como parte determinante en la toma de decisiones que afecten derechos de las personas;

9) no realizar 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, tomar los recaudos necesarios según el caso para verificar su legalidad (informe de auditoría, dictamen previo, etc.);

11) tanto el 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 Nº 25.326 y el Anexo I del Decreto Nº 1558/2001[38];

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 Nº 1558/2001.

7. Conclusiones

En la actualidad, 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 de 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 se debe entender que la protección de principios como los de limitación de la finalidad y la minimización de datos es fundamental para garantizar la privacidad de las personas, especialmente en contextos donde se recopila una cantidad cada vez mayor de información sobre los individuos.

A su vez, tecnología e ingeniería conscientes de la privacidad serán variables importantes para asegurar la transparencia y el control de los datos por los usuarios. Tanto leyes, regulaciones, bunas prácticas, normas corporativas, cláusulas contractuales, si bien son importantes, no son suficientes por sí solas. Es necesario ofrecer a las personas nuevas e innovadoras maneras de ser informados acerca de lo que ocurre con sus datos y que ellas puedan ejercer el control. Esto requiere tecnología y procesos de ingeniería innovadores y de fácil uso, así como disposiciones organizativas y modelos de negocios respetuosos de la intimidad. Una ingeniería innovadora y responsable deberá facilitar, entre otros, el ejercicio de los derechos de acceso, supresión, actualización, así como también el de confidencialidad.

Otro factor que aporta 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, 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.

Como futura línea se trabajará en la definición de un proceso de análisis que permita describir y evaluar la reglamentación local vigente referida a la protección de datos personales en proyectos de Big Data. El proceso de análisis propuesto buscará identificar y valorar el grado de cumplimiento con la normativa local, lo que facilitará la toma de decisiones informadas, basadas no solo en criterios técnicos o económicos, sino también regulatorios.

Referencias

1. Castells, M.: La era de la información. Economía, sociedad y cultura. Vol. 1 La sociedad red. (2ª edición). Madrid, Alianza. (1997) 456-463
2. Castells M.: Conferencia inaugural del programa de Doctorado sobre la Sociedad de la Información y el Conocimiento en la Universidad Abierta de Cataluña. Internet y la Sociedad red. (2000) [Online] Disponible en: http://goo.gl/NJecTA (Recuperado el 4 de Mayo de 2016)

3. Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. & Byers, A. H.: Big Data: The Next Frontier for Innovation, Competition, and Productivity. McKinsey Global Institute. (2011) 15-27
4. Brynjolfsson, E., Hitt, L., Kim, H. H.: Strength in Numbers: How Does Data-Driven Decision making Affect Firm Performance. ICIS 2011Proceedings, Shangai. (2011) 4-7
5. United Nations Global Pulse 2012. "Big Data for Development: Challenges & Opportunities" United Nations. (2012) 35-39
6. Chen, C. L., & Zhang, C. Y.: "Data-Intensive Applications, Challenges, Techniques and Technologies: A Survey on Big Data. Information Sciences 275. (2014) 314-347
7. Nissenbaum, H.: Protecting Privacy in an Information Age: The Problem of Privacy in Public, 17 LAW & PHIL. (1998) 559
8. Asamblea General de las Naciones Unidas: The Right to Privacy in the Digital Age, Res. 69/166. Doc. (A/RES/69/166) (2014)
9. Camargo Vega, J.J., Camargo Ortega, J.F., Joyanes Aguiar: Conociendo Big Data. Revista de Ingeniería, Facultad de ingeniería Universidad de La Rioja, Vol. 24, n. 38. (2015) 63-77
10. Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. & Byers, A. H.: Big Data: The Next Frontier for Innovation, Competition, and Productivity. McKinsey Global Institute. (2011) 15-27
11. Beyer M., Laney, D.: The importance of big data: A definition. Gartner Publications. (2012) 1-9
12. ITU-T Study Group 13: Big data – Cloud computing based requirements and capabilities Recommendation Y.3600. (2015) 1-2
13. World Economic Forum: Big Data, Big Impact: New Possibilities for International Development. (2012) [Online] Disponible en: http://goo.gl/ZVIjQC (Recuperado el 22 de Abril de 2016)
14. International Working Group on Data Protection in Telecommunications: Working Paper on Big Data and Privacy Privacy principles under pressure in the age of Big Data analytics. 55th Meeting, Skopje (2014) 1-5
15. European Data Protection Supervisor: 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. (2014) 6-8
16. Gonzalez F. G., Scherrer A.: Big Data and smart devices and their impact on privacy. European Parliament. Directorate General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs (2015) 10-14
17. Segura, P.: Internet de las Cosas. En Travieso, J. A. (Director) Régimen jurídico de los datos personales, Tomo I. Ed. La Ley. Buenos Aires (2014) 521-537
18. Evans, D.: The Internet of Things: How the Next Evolution of the Internet Is Changing Everything. Cisco Systems. (2012) [Online] Disponible en: http://goo.gl/ivhZdT (Recuperado el 21 de Abril de 2016)
19. Piyare, R.: Internet of Things: Ubiquitous Home Control and Monitoring System using Android based Smart Phone. International Journal of Internet of Things, Vol. 2, No. 1. (2013) 5-11
20. Bandyopadhyay, D., Sen, J: Internet of Things - Applications and Challenges in Technology and Standardization, Wireless Personal Communications. Vol. 58, Issue 1. (2011) 49-69
21. Velosa, A., Hines, J. F., Hung, L. H., et al.: Gartner Predicts 2015: the Internet of Things. (2014) [Online] Disponible en: https://goo.gl/Tr88tp. (Recuperado el 25 de Marzo de 2016)
22. Mitchell, S., Vila, N., et al.: Connecting People, Process, Data, and Things to Improve the 'Livability' of Cities and Communities. Cisco Systems. (2013) 4-5
23. International Conference of Data Protection and Privacy Commissioners: Mauritius Declaration on the Internet of Things. 36th International Conference of Data Protection and Privacy

Commissioners. (2014) [Online] Disponible en: http://goo.gl/I3Kgbn (Recuperado el 19 de Abril de 2016)
24. Wheatley, M.: Big Brother's Big Data: Why We Must Fear The Internet Of Things? (2013) [Online] Disponible en: http://goo.gl/yNQyWO (Recuperado el 8 de Mayo de 2016)
24. Mell P., Grance T.: The NIST Definition of Cloud Computing. National Institute of Standards and Technology, U.S. Department of Commerce. NIST Special Publication 800-145 (2011) 2-3
25. Gonzalez Allonca, J.C., Piccirilli, D. & Pollo-Cattaneo M.F. : Modelo de Análisis Relativo a la Protección de Datos Personales para Proyectos de Cómputo en la Nube. Proceedings XVIII Workshop de Investigadores en Ciencias de la Computación (WICC 2016). Workshop de Seguridad Informática. Artículo 8737. (2016)
26. Gonzalez Allonca, J.C., Piccirilli, D.: Consideraciones Legales Relativas a la Privacidad en Proyectos de Cloud Computing en el Exterior de Argentina. Revista Latinoamericana de Ingeniería de Software, Vol. 2, No. 1. (2013) 86-87
27. World Economic Forum: The Global Information Technology Report 2014 - Rewards and Risks of Big Data. (2014)
28. Asamblea General de las Naciones Unidas: The Right to Privacy in the Digital Age, Res. 69/166. Doc. (A/RES/69/166) (2014)
29. Bąkowski, P.: Big data: opportunities and privacy concern. Research Service European Parliamentary. (2014) 2
30. Polonetsky, J., Tene, O.: Privacy and Big Data: Making Ends Meet. Stanford Law Review, Vol. 66, No. 25. (2013) 120-121
31. Duhigg, C: How companies learn your secrets. New York Times. (2012) [Online] Disponible en: https://goo.gl/ZTLdPW (Recuperado el 5 de Mayo de 2016)
32. Hoffman, S.: Medical Big Data and Big Data Quality Problems. 21 Connecticut Insurance Law Journal 289; Case Legal Studies Research Paper No. 2015-18. (2014) 303-305
33. Bruce E., Sollins K., Vernon M., Weitzner D.: Big Data Privacy Scenarios. Computer Science and Artificial Intelligence Laboratory Technical Report. Massachusetts Institute of Technology. (2015) 41-43
34. Terhune, C.: They Know What's in Your Medicine Cabinet, Bloomberg Businessweek. (2008) [Online] Disponible en: http://goo.gl/DU3VhI (Recuperado el 5 de Mayo de 2016)
35. Ley N° 25.326 (2000) Ley de Protección de Datos Personales. Boletín Oficial de la República Argentina.
36. Agencia de Informática y Comunicaciones de la Comunidad de Madrid: Procedimiento de disociación de datos personales. (2011) [Online] Disponible en: http://goo.gl/NoCTkS (Recuperado el 7 de Mayo de 2016)
37. Grupo de Trabajo sobre Protección de Datos del Artículo 29 (WP29): Dictamen 05/2014 sobre técnicas de anonimización. (2014) [Online] Disponible en: http://goo.gl/ZcBwn7(Recuperado el 21 de Abril de 2016)
38. Decreto 1558 (2001) Reglamentación de la Ley N° 25.326. Boletín Oficial de la República Argentina.