Universidad Siglo XXI

El derecho a la intimidad, la protección de datos personales y el *big data* a la luz del ordenamiento jurídico argentino

Trabajo final de grado

Carrera: Abogacía

Autora: Silvia Rosana Hoferek

Legajo: VABG62612

Tutor: Pablo Maffrand

2019

Resumen

La investigación se enmarca en las áreas del derecho público y del derecho privado, siendo tratadas las ramas del derecho constitucional y del derecho informático respectivamente.

El tema abordado será el derecho a la intimidad, la protección de datos personales y el big data a la luz del ordenamiento jurídico argentino, en especial a partir de la Constitución Nacional y los principios establecidos en la ley 25.326. Inquiriendo específicamente sobre ¿Cuál es el alcance de la ley 25326 de protección de datos personales en relación al supuesto de uso del denominado big data? y ¿Bajo qué argumentos normativos el big data entraría en tensión con el derecho a la intimidad y a la protección de los datos personales?

Palabras clave

Derecho a la intimidad. Datos personales. Big data. Principios. Hábeas data.

Abstract

It is framed within the area of public law as well as private law, being treated the branch in constitutional law and the computer law.

The topic addressed will be the right to privacy, the protection of personal data and big data in light of the Argentine legal system, especially based on the principles established in law 25.326. Inquiring: What is the scope of law 25.326 on the protection of personal data in relation to the assumption of the use of the so-called big data? and under what normative arguments does big data come into tension with the right to privacy and the protection of personal data?

Key words

Right to privacy. Personal data. Big data. Principles. Hábeas data.

Índice

Introducción

El objetivo del presente trabajo es establecer el alcance de la ley 25.326 de protección de datos personales en relación al supuesto del uso del denominado big data, y determinar bajo qué argumentos normativos el big data entraría en tensión con el derecho a la intimidad y la protección de los datos personales.

El tema propuesto se encuentra comprendido, por un lado, en la rama del derecho Constitucional dentro del derecho público, puesto que tanto el derecho a la intimidad, como la protección de datos personales, se encuentran en los artículos 19[1] y 43, párrafo 3º[2] de nuestra Constitución; y por el otro, el derecho informático, rama perteneciente al derecho privado.

Esta investigación será guiada por los siguientes interrogantes ¿Cuál es el alcance de la ley 25.326 de protección de datos personales en relación al supuesto del uso del denominado big data? y ¿Bajo qué argumentos normativos el big data entraría en tensión con el derecho a la intimidad y a la protección de los datos personales?

La hipótesis que se plantea es que el uso del big data entraría en tensión con el derecho a la intimidad y la protección de datos personales cuando incumple los principios establecidos en la ley 25.326, requiriendo una respuesta del ordenamiento jurídico argentino a través de la acción de protección de datos personales, denominada hábeas data.

El contenido estará estructurado en cuatro capítulos, a través de los cuales se abordarán el derecho a la intimidad, la protección de datos personales y sus principios, el big data y la acción hábeas data.

En el primer capítulo, se conceptualizará normativa, jurisprudencial y doctrinariamente el derecho a la intimidad, se caracterizará dicho derecho y se determinará el bien jurídico protegido, incluyendo los datos personales. En el segundo apartado se analizarán el alcance de los datos personales desde el derecho a la intimidad y los aspectos que los definen según la ley 25.326. Se describirán las tipologías, el objeto de la ley y se contextualizará su tratamiento en el marco normativo. También se caracterizará y conceptualizará el hábeas data.

---

[1] Constitución de la Nación Argentina (1994), Artículo 19: Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados...

[2] Constitución de la Nación Argentina (1994), Artículo 43, Párrafo 3º: Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.

En el capítulo siguiente, se analizarán los principios de la ley 25.326, sus objetivos, el alcance y en que consiste cada uno de ellos, cuáles son las dificultades de su aplicación y los aspectos en los que se ven afectados por los procedimientos de big data.

El capítulo tres se aboca al conocimiento del big data, su conceptualización en el ámbito tecnológico, caracterización a través de las cinco V, y la aplicación de los principios de protección de datos personales a esta actividad. Se delimitará el área del big data que interesa a este trabajo: los datos relacionados a las personas.

Por último, en el capítulo cuatro, se analizarán la acción de protección, los tipos previstos por la ley y la doctrina, y fallos de importantes tribunales nacionales como la corte Suprema de Justicia de la Nación y la Cámara Nacional de Apelaciones Civil y Comercial de la Nación, entre otros.

El desarrollo del tema se basará en la legislación, doctrina y jurisprudencia seleccionadas como fuentes primarias y secundarias de este trabajo, tales como la ley 25.326 de protección de datos personales, la Constitución nacional, el Código Civil y Comercial, trabajos de reconocidos autores y fallos seleccionados. La metodología a utilizar será descriptiva-exploratoria de corte cualitativo, porque se examinarán y explorarán detalladamente procesos o contextos para comprender el fenómeno social concreto de protección de la intimidad y de los datos personales.

Se elige esta metodología, porque es la que mejor se adapta al dinamismo que caracteriza a la legislación en el mundo moderno y la que permitirá realizar un análisis profundo y crítico de la dimensión normativa y valorativa de los fenómenos jurídicos mencionados. La temática a desarrollar está constantemente ampliando sus campos, con circunstancias y situaciones emergentes y con la necesidad de brindar soluciones a problemáticas jurídicas surgidas por el uso de nuevas tecnologías. Es por ello que también se estudiaran autores del área tecnológica donde encontraremos definiciones y conceptos novedosos y actuales de big data.

Capítulo I

El derecho a la intimidad, los datos personales y el hábeas data

Prefacio

En este capítulo se conceptualizarán normativa, doctrinaria y jurisprudencialmente el derecho a la intimidad, los datos personales y la acción de protección, llamada hábeas data, a fin de establecer las bases para responder los interrogantes ¿Qué es el derecho a la intimidad?, ¿Qué son los datos personales? y ¿En qué consiste el hábeas data?

Para ello se extraerán los conceptos de la Constitución Nacional, el Código Civil y Comercial Argentino, la ley 25.326 y especificaciones de importantes autores, a los que se sumarán definiciones de la jurisprudencia nacional.

Además, se caracterizará a cada uno de estos conceptos, analizando sus puntos principales como el bien jurídico tutelado, sus tipologías, su relación con los derechos personalísimos y la protección brindada por la legislación argentina y por tratados internacionales a los que nuestro país adhiere.

1. Derecho a la intimidad

1.1 Conceptualización

En el derecho argentino, la tutela legal del derecho a la intimidad se encuentra en el artículo 19 de la Constitución Nacional, primera parte, donde expresa que las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados.

También en el artículo 75, inciso 22, de la Constitución Argentina, nuestro país reconoce y adhiere a tratados internacionales que debe respetar. El derecho a la intimidad se protege en el Pacto Internacional de Derechos Humanos Civiles y Políticos, en su artículo 17, en los incisos 11 y 12 del artículo 11 de la Convención Americana de Derechos Humanos, como así también en la Declaración Universal de los Derechos Humanos, en su artículo 12, donde prescribe que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación y que la ley debe proveer su protección.

El ex presidente de la Corte Suprema de Justicia de la Nación, Ricardo Lorenzetti, al momento de explicar el nuevo Código Civil y Comercial de la Nación, manifestó que el capítulo 3 se refiere a los derechos personalísimos, y menciona que son los que protegen al individuo frente a los avances tecnológicos y económicos que producen la intromisión en la vida privada de las personas, usando su imagen, manipulando sus datos

personales y sensibles y su información médica. Ante esto los derechos personalísimos garantizan su resguardo (Lorenzetti, 2015).

En el Código Civil y Comercial, ley 26.944, el tratamiento del derecho a la intimidad, se encuentra en el capítulo 3, Derechos y Actos Personalísimos, del Libro primero, donde se incluyen el derecho a la intimidad y la necesidad del consentimiento informado, artículos 52, 53 y 55.

Teniendo en cuenta estos conceptos se podría concluir que los datos personales particulares, sensibles y propios forman parte de la intimidad personal y por lo tanto gozan del derecho a su protección a través del derecho a la intimidad, establecido en el artículo 19 de nuestra Constitución Nacional, el hábeas data incorporado en el artículo 43, tercer párrafo de dicha Constitución y la ley 25.326 de protección de datos personales.

1.2 Caracterización del derecho a la intimidad

El derecho en análisis, es un derecho personalísimo, por lo tanto, se caracteriza por ser innato, vitalicio, imprescindible e inalienable, puesto que corresponden al titular desde el origen de éste, lo acompañan toda su vida, no es alcanzado por efecto del tiempo, no influye en su pérdida y está fuera del comercio. También, es absoluto, pues se ejerce erga omnes y, por último, es privado puesto que depende de cada sujeto (Llambías, 1997).

1.3 Bien Jurídico tutelado

Los derechos personalísimos se convierten en bienes jurídicamente protegidos. La persona puede disponer de esos bienes mientras no sean contrarios a la ley, la moral y las buenas costumbres. Aprobar la divulgación de su imagen; autorizar la realización de tratamientos médicos, clínicos o quirúrgicos; donar un órgano; permitir la publicación de una autobiografía o de una nota periodística que difunda detalles personales son actos que requieren consentimiento de su titular. El consentimiento no se presume. Esto quiere decir que, en caso de la violación de un derecho personalísimo, si no hay pruebas de lo contrario, la justicia supondrá que no existió el consentimiento. Los datos personales forman parte de los bienes tutelados a través de los artículos 19 y 43, inciso 3, de nuestra Constitución Nacional.

La incorporación de los artículos 52[3] y 1770[4] realizada por la ley 26.944, es decir el Código Civil y Comercial, era necesaria, debido a que la tecnología avanza cada vez más, y junto con este avance aparecen muchos casos que infringen los derechos personalísimos, como la divulgación de imágenes o datos personales sin autorización y la violación de la intimidad, por medio de las redes sociales, medios públicos, entre otros.

En este sentido el Código civil y comercial, establece una faz preventiva, que consiste en una facultad atribuida a la persona afectada, para que cesen las actividades dañosas, así como una faz resarcitoria para obtener una reparación plena a favor del damnificado (Herrera, Caramelo, Picasso, 2015).

Según la interpretación realizada por estos últimos autores, el elemento primordial para que el damnificado pueda utilizar los recursos disponibles es que exista un entrometimiento arbitrario en su vida por parte del sindicado. Es decir, "…si se tratara del ejercicio regular de un derecho o el cumplimiento de una obligación legal no resulta de aplicación el art. 1770 CC y C "(Herrera, Caramelo, Picasso, 2015, p.500), así como tampoco si se contara con el consentimiento informado y libre del ofendido.

La ilicitud entonces, se ve determinada por la arbitrariedad en la manipulación y tratamiento de los datos sin contar con el derecho correspondiente.

2. Datos Personales

2.1 Concepto

Los datos personales son definidos por la ley 25.326, en su artículo 2, como información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. Estos también comprenden, según dicho artículo, los datos sensibles que son aquellos que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

[3] Artículo 52 Código Civil y Comercial de la Nación: "La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos…"

[4] Artículo 1770 Código Civil y Comercial de la Nación: "Protección de la vida privada. El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias. Además, a pedido del agraviado, puede ordenarse la publicación de la sentencia en un diario o periódico del lugar, si esta medida es procedente para una adecuada reparación".

Según el Reglamento general de protección de datos de la Unión Europea, vigente desde mayo del 2018, en su artículo 4, los datos personales están conformados por cualquier información relativa a una persona física viva identificada o identificable. También constituyen datos personales, toda información que compilada o procesada permita identificar a una persona determinada. Tales el caso de aquellos que habiendo atravesado procesos de anonimización, cifrado, encriptados o con seudónimo, aún puedan reconstruir un conjunto de datos que definan unívocamente a una persona (Reglamento europeo, 2016).

Contrariamente, si estos últimos procesos fueron eficientes al no permitir la identificación de personas y además dicho proceso es irreversible, estos datos dejarán de considerarse personales.

Este Reglamento de la Unión Europea, protege los datos personales independientemente de la tecnología utilizada para su tratamiento; es decir es tecnológicamente neutro y se aplica tanto al tratamiento automatizado como manual. En cuanto a su conservación, no diferencia su forma o medio, ya sea en un sistema automatizado de información, a través de video vigilancia o sobre papel, los datos personales están sujetos a la aplicación del Reglamento mencionado.

La Argentina debe cumplir con las normas de este Reglamento, siempre que se encuentre relacionada por alguna transferencia internacional de datos, o se cedan algunos de ellos, o a través de empresas u organismos por diferentes intercambios, culturales, comerciales, económicos, científicos o tecnológicos. Es una de las razones por la cual se encuentra presentado el proyecto de la nueva ley de protección de datos personales en el Congreso Nacional mediante el mensaje 147/18.

El Reglamento europeo trata la transferencia de datos personales a terceros países u organizaciones internacionales en el capítulo V, Artículo 44, donde describe el principio general de transferencias.

2.2 Caracterización

Los datos personales son información de cualquier tipo que pueda ser usada para identificar, contactar o localizar a una persona (Ques, 2014).

Entre ellos se encuentran nombre y apellido, número de documento, nacionalidad, sexo, estado civil, número de teléfono y/o celular, huellas digitales, dirección de correo electrónico, ubicación espacial, actividades, opiniones, etcétera. En nuestra vida cotidiana, todos compartimos diferentes tipos de datos que hacen a nuestra identidad y

nuestras cualidades personales, tanto de forma presencial como de manera digital o a través de datos biométricos.

El artículo 4 del Reglamento europeo de protección de datos personales, describe a los datos personales como toda información sobre una persona física identificada o identificable.

Esta persona que el mismo artículo denomina interesado, es aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Al realizar trámites en organismos públicos o privados, al publicar contenidos en redes sociales, al descargar aplicaciones en los dispositivos móviles, cuando se realizan compras en línea o completan encuestas, entre muchas otras actividades, estamos brindando información personal de manera voluntaria, puesto se realiza personalmente o a través de las políticas de privacidad y aceptando condiciones de los sitios correspondientes en internet. En la web circulan los datos personales que se comparten en las redes sociales, en los sitios frecuentados, en formularios digitales, en sitios de juegos y de compras. Éstos datos se brindan de forma voluntaria y con conocimiento, expresados a través del consentimiento y en concordancia con el decreto 1558/01 y sus modificatorias dispone en su artículo 5 que 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 6 de la ley 25.326.

Pero también circulan otros datos que muchas veces se desconocen. Entre ellos, las informaciones de patrones de navegación y comportamiento en la red y los datos que otras personas difunden en la web sin el conocimiento, sin autorización del propietario, o sin contar con ninguno de los dos, pero como forman parte del círculo de amistades prevalece la confianza. Todo esto conforma una reputación web, que es toda la información disponible en internet relacionada a la a identidad particular de una persona.

La identidad digital se configura a partir de los contenidos accesibles a través de medios electrónicos y, por tanto, empieza a crearse desde el primer rastro que se deja en Internet, que no tiene por qué haber sido dejado por la propia persona (Gamero Casado, 2011). Los foros y redes sociales de Internet están repletos de datos personales publicados por usuarios que, en la mayoría de los casos, no son titulares de los mismos y, salvo que

dicha página de destino no sea rastreable por buscadores, la información volcada es fácilmente accesible a través de buscadores.

Según Lezcano, el uso de las nuevas tecnologías, principalmente Internet, trajo como consecuencia que una gran parte de los datos personales pasaron la esfera de lo privado para convertirse en muchos casos, en datos de acceso público, y con el uso de las redes sociales este fenómeno se ha ido incrementando (2010). Este intercambio electrónico de datos, conforma la identidad digital personal, y se configura cuando un conjunto de datos personales se asocia a una entidad humana en el marco digital (Sullivan, 2011).

2.3 Tipos

La ley 25.326, en su artículo 2, define datos personales, así como también brinda un concepto de datos sensibles mencionando que estos son los que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

De acuerdo a esta definición podemos distinguir que existen otras clasificaciones de datos según sus características, que detallaremos a continuación.

Los de identificación permiten determinar unívocamente, solos o en conjunto, a una persona. Podemos mencionar entre ellos el nombre, el apellido, el domicilio, el código único de identificación laboral, la fecha de nacimiento, la nacionalidad, el número de documento, entre otros, que son registrados y almacenados en las bases de datos del Registro nacional de las personas, organismo dependiente del Ministerio de Interior de la Nación.

Los datos laborales se relacionan con la actividad que realizan las personas para lograr una subsistencia económica para ellas y su familia, tales como puesto, salario, cargo, legajo, sanciones, la empresa para la cual trabaja y su ubicación geográfica, los mismos se encuentran enumerados en el artículo 52 de la ley 20.744, de contrato de trabajo.

Los patrimoniales representan los bienes materiales de una persona o se su familia. Conforman el acervo personal y familiar y cuentan con numerosas leyes que los protegen. Podemos mencionar la situación crediticia y financiera a través del artículo 39 de la ley 21.526, de entidades financieras, así como también la misma ley protege a través del secreto fiscal todos los datos referentes a la posición fiscal, inmuebles, haberes, muebles, entre otros, que el contribuyente brinde en sus declaraciones juradas o, que según la ley

11.385 de procedimiento fiscal, la Administradora fiscal de ingresos públicos pueda recolectar en cumplimiento de su artículo 35.

Los datos de formación permiten establecer la trayectoria académica, educativa y de formación resguardando los referidos a historia educativa, títulos, número de cédula, certificados, nivel de instrucción, que, dependiendo del ámbito nacional, provincial, o privado se resguarda en bases debidamente inscriptas en el Registro nacional de bases de datos o se archivan según Decreto 1131/2016 del Poder ejecutivo, de mantenimiento de expedientes y tiempo de resguardo de archivos.

Otro grupo especialmente sensible es el de los datos ideológicos, tales como creencias religiosas, afiliación política o sindical, pertenencia a organizaciones de la sociedad civil o asociaciones religiosas, salvo para usos internos de las respectivas asociaciones tal como lo expresa el inciso 3 del artículo 7 de la ley 25.326.

También se encuentran los datos de salud, que son sensibles y protegidos por la relación profesional-paciente a través del resguardo de su historia clínica en la cual se detallan enfermedades, cuadros sicológicos, psiquiátricos, tratamientos y especialmente tutelados por la ley 25.326 y constituyen un deber ético de esta relación.

Los datos de características personales como tipo de sangre, ADN, huella digital, y los de cualidades físicas como color de piel, iris y cabellos, señales particulares, también forman parte de los datos protegidos por la ley 25.326, pero hasta la actualidad no se los considera sensibles. En el nuevo proyecto de ley presentado con el mensaje 147/2018 del Poder Ejecutivo, estos datos se denominan biométricos y pasarían a formar parte de los datos sensibles.

En cuanto a las costumbres, vida y hábitos sexuales, origen étnico y racial, están especialmente protegidos ya que su uso indebido provoca males propios de la época como acoso, maltrato en las redes o bullying, y discriminación (Gozaíni, 2011).

El Reglamento europeo de protección de datos personales define especialmente ciertos datos considerados sensibles. Entre ellos, en el artículo 4, apartado 13, se refiere a los datos genéticos que son los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Por otra parte, en el mismo artículo, apartado 14, define que los datos biométricos son los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan

o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Por último, en el apartado 15 se encuentra la definición de los datos relativos a la salud, en la que enuncia que son los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

La ley 35.426, define a los datos relativos a la salud y a los sensibles, pero nada dice acerca de los datos genéticos ni de los biométricos.

En el 2011, se sancionó el Decreto 1.766 que crea el Sistema Federal de Identificación Biométrica para la Seguridad. Es un hito en la utilización de la biometría a los efectos de comprobar la identidad de una persona. A partir de la puesta en marcha del sistema informático será posible la comparación y análisis fisonómico de una persona respecto de una base de datos con archivos históricos y actualizables creada y administrada para la identificación.

En el proyecto de la nueva ley de protección de datos personales se incorpora este tipo de datos, y así se regula a fin de concordar con el Reglamento europeo para la trasferencia internacional de datos. Aún sin aprobarse la ley, el sistema biométrico se expande y amplía su utilización en la AFIP, padrones electorales, cajeros automáticos, aeropuertos, por mencionar algunos.

2.4 Bien jurídico tutelado. Objeto de la ley

El derecho a la intimidad, entendido como garantía de un ámbito reservado, frente a injerencias de terceros, y la protección de la imagen y el honor son bienes jurídicos tutelados por la ley de protección de datos personales (Gozaíni, 2006). Dicha ley, en su artículo 1, indica que su objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad y permitirle el acceso a la información que sobre las mismas se registre.

A fin de ordenar y controlar los datos personales, las bases de datos deben inscribirse en el Registro nacional de bases de datos personales. El artículo 21 de la ley 25.326 dispone que todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control, que es la Dirección nacional de protección de datos personales.

Es de resaltar también, que en el mensaje 147/18 del Poder ejecutivo, se destacan las nuevas regulaciones europeas, reconociendo un nuevo contexto internacional que dio fundamento al Reglamento (UE) 2016/679 del Parlamento europeo y del consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En dicho mensaje el Poder ejecutivo nacional resalta que la Argentina "…desde el año 2003 es considerada por la Unión europea como un país con legislación adecuada para la protección de los datos personales…" y la importancia de mantener nuestra legislación afín con esos estándares internacionales para conseguir nuevas posibilidades de innovación e inversión en nuestro país (Poder ejecutivo, 2018).

3. Hábeas data

3.1 Contextualización

El uso de la tecnología sin los parámetros de seguridad o mediante delitos puede generar daños en la privacidad e intimidad de las personas con un alto costo de reparación, y si, como Bidart Campos (1998) explica, el hábeas data significa que cada persona tiene sus datos, es necesario protegerlos. Es por ello que los gobiernos se ocupan de producir leyes que brinden dicha protección. La Declaración Universal de los Derechos Humanos (1948), en su artículo 12, refiere que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, y que, en caso de injerencias o ataques, toda persona tiene derecho a la protección de la ley.

En nuestro país, el hábeas data constituye, desde 1994, una garantía constitucional regulada a través de la acción de amparo en el Artículo 43, tercer párrafo, de la Constitución Nacional. Posteriormente, en el año 2000 se sancionó la ley 25.326, norma de orden público, que regula los principios aplicables en la materia y el procedimiento de la acción de hábeas data. El 19 de septiembre de 2018, el Proyecto de la nueva ley de protección de datos personales fue presentado al Congreso Nacional mediante el mensaje 147/2018 del Poder Ejecutivo[5], incluyendo las reformas que con urgencia demanda la ley

[5] Mensaje 147/18 del Poder ejecutivo recuperado de https://www.argentina.gob.ar consultado en septiembre 2018

vigente, tanto por el aumento de vulnerabilidades ante el avance de la tecnología, entre ellas el big data, como para adecuarla a estándares europeos.

Las provincias también incorporaron en sus constituciones el hábeas data. La de Córdoba en el artículo 50, la de Buenos Aires en el artículo 20, inciso 3. La ciudad de Buenos Aires suma esta garantía en el artículo 10 de su Constitución y a través de la Ley 1845.

3.2 Concepto

El hábeas data en el ámbito público, es definido por Sánchez Bravo (2001) como una garantía de los derechos de los ciudadanos ante el manejo discriminatorio de la información almacenada o tratada informáticamente por parte del poder público.

Según el Diccionario judicial español, dependiente de la Real Academia Española, el hábeas data tiene dos acepciones. La primera dice que es la "acción constitucional que puede ejercer cualquier persona incluida en un registro de datos para acceder al mismo y recabar la información que le afecte, así como solicitar su eliminación o corrección si tal información fuera falsa o estuviera desactualizada". La segunda, referida a al derecho informático, define al hábeas data como el "derecho a la propia intimidad informática, que confiere a su titular un derecho de control sobre los datos (acceso, rectificación y cancelación de los mismos) …" (Diccionario del Español Jurídico, 2016). Ambas acepciones son receptadas por la ley 25.326.

El fundamento de la garantía que tutela el hábeas data, es la defensa de los derechos tales como el honor, la reputación, la privacidad y la imagen, entre otros, cuyo género es el derecho a la intimidad, del cual forman parte los datos personales. La acción autónoma de hábeas data es el recurso legal con el que cuenta su titular cuando encuentra dificultades para el ejercicio del derecho a la protección de los mismos, o se deniegue u omita su derecho (Puccinelli, 2014).

La protección brindada por el hábeas data abarca además la vigilancia de las telecomunicaciones, las cuales sólo pueden realizarse con orden judicial fundada según el artículo 18 de la ley 19.798 de telecomunicaciones, también tiene alcance en cuanto a datos biométricos que sean utilizados para determinar sexo, religión, raza u otro elemento que pueda ser discriminatorio, o para cualquier uso no consentido que perjudique de manera inminente la intimidad, el honor o la reputación de una persona. Las redes sociales en sus páginas de Políticas de privacidad y condiciones de uso brindan información acerca del responsable, lugar donde se almacenan los datos, seguridad, entre otras, y detallan que

ante la solicitud del titular los datos se eliminarán, pero que no se hacen responsables si ya otras redes o sitios bajaron la información y la utilizan sin autorización (Pérez Sanz, 2016).

3.3 Autonomía

En la Argentina, la autonomía del hábeas data tiene un desarrollo propio logrado con el artículo 43 de la Constitución Nacional y regulado por una ley especial. Esta autonomía, como proceso diferente al amparo, se sostiene por la identidad propia del objeto a demandar. En nuestro país no existe el amparo contra los actos arbitrarios o ilegítimos que en forma actual o inminente afecten la libertad por el uso de datos personales. La vía pertinente es el hábeas data como actual mecanismo para lograr el acceso a archivos y otras pretensiones como la actualización, rectificación, supresión, confidencialidad; inclusive con la ley se puede responder a lesiones derivadas al honor, la intimidad o la reputación, entre otras (Gozaíni, 2006).

Es importante agregar que la rapidez con la que se instrumenta esta acción, aumenta las posibilidades de protección, ya que, si es expuesto un dato sensible o perjudicial, cuanto mayor tiempo permanezca publicado hay mayor posibilidad de transmisión y uso indebido, y menor posibilidad de reparación. Muchas de las páginas web y redes sociales, tales como Google, Facebook, Instagram, Amazon, entre otras, advierten al usuario, en sus condiciones de uso, que los datos allí expuestos por su titular presuponen que el mismo quiere que se publiquen, de lo contrario dicho titular debe solicitar su supresión.

Hay otros datos que se guardan sin que los usuarios de internet se den cuenta, tal es el caso de Google, como páginas visitadas frecuentemente, tiempo que se pasa en ellas, ubicación, sitios recientes, y otras que podrían permitir definir perfiles de los usuarios. Ante cualquiera de estos usos indebidos o dañosos la acción a ejercer es el hábeas data (Doan., Halevy & Ives,2012).

En cualquiera de los casos de vulneración del derecho a la intimidad y al uso no consentido de los datos personales, Morello (2003) explica, que el hábeas data es la vía directa para comunicarse con los jueces, y obtener la debida protección de los derechos y garantías constitucionales menoscabados o amenazados. La acción de hábeas data es protectora y autónoma pues se identifica con todos sus elementos esenciales, procedimientos propios y un bien tutelado determinado.

3.4 El hábeas data y su relación con el derecho a la intimidad y los datos personales

Los datos personales son parte de los bienes protegidos por el derecho a la intimidad. A través del artículo 43 de la Constitución Nacional logran una protección mayor y específica mediante el hábeas data. El tercer párrafo de dicho artículo, derivó en la sanción de la ley 25.326, en cuyo texto desarrolla detalladamente la acción de hábeas data. En cuanto a nuestro tema refiere, su relación con el big data, se deben conciliar adecuadamente la preeminencia del respeto a los derechos del hombre con el de la libertad de información entre los pueblos a fin de alcanzar el desarrollo económico y social.

La ley protege la información perteneciente a las personas con domicilio legal en nuestro país, según el artículo 2 de la ley 25.326[6] , excluyendo a datos que existen en embajadas y consulados, y a los referidos a datos entre sociedades con empresas que actúan en el exterior. Como las disposiciones de la ley 25.326, artículo 1, se aplican a los a los bancos de datos destinados a dar informes podría ocurrir que empresas de un mismo grupo económico intercambien datos, con establecimientos propios en países cuya legislación no provea la suficiente protección.

Los derechos que reconoce la ley de protección de datos personales pueden ejercerse en el ámbito de Internet (Palazzi, 2004). La dificultad de su ejercicio está basada en la posibilidad de determinar el lugar donde se originó ese sitio de Internet al que le proporcionamos u obtiene nuestros datos, la escasa posibilidad de identificar al titular de una página web, la diversa y cambiante cantidad de legislaciones locales, nacionales y en el mundo sobre el tema, y la aceptación expresa o tácita de las políticas de privacidad de algunos sitios a los que los usuarios muy pocas veces atienden, o, incluso como lo advierte Ferreyra (2018), que se presentan en idioma diferente al nacional o determinando una jurisdicción y norma de aplicación extranjeras.

Conclusión Parcial

En este capítulo se realizó una descripción detallada de los conceptos claves en los que se centra el trabajo. Se conceptualizaron doctrinaria, jurisprudencial y normativamente el derecho a la intimidad, los datos personales y el hábeas data.

[6] Artículo 2 (Definiciones) Ley 25346: "…Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley…"

En cuanto al derecho a la intimidad, específicamente se hizo referencia a su tratamiento en la constitución nacional, y su caracterización como parte de los derechos personalísimos, protegido tanto por el artículo 19, como por el artículo 75, inciso 22, con la incorporación de tratados internacionales a nuestra carta magna.

El derecho a la intimidad se ve expuesto, algunas veces, a través de datos personales, contenidos en bases de datos, por lo que en este capítulo también se proporciona la definición según la ley 25.326, sus características y clasificación normativa y doctrinaria, exponiendo a la vez, el objeto de la ley.

Por último, se realiza una introducción al hábeas data contextualizándolo en la actualidad según la doctrina, proporcionado su concepto y referenciando su relación con el derecho a la intimidad y los datos personales, según los artículos 19 y 43 de la Constitución Nacional.

Si bien la Constitución Nacional y la ley de protección de datos personales definen claramente el objeto y la finalidad con la que los datos deben ser colectados, hay una gran cantidad de procesos y procedimientos que no cumplen con dichas normas, sobre todo los que tratan con datos masivos como el big data. El ordenamiento jurídico en su afán de protección no debería limitar los avances científicos ni tecnológicos, ni paralizar las operaciones que se vean favorecidas con estas tecnologías, sino mejorar sus controles y brindar mayores garantías en su protección.

Capítulo II

Principios de la ley 25.326

Prefacio

Los principios de protección de datos personales contemplados en el capítulo dos de la ley 25.326, establecen el marco regulatorio para la manipulación de datos personales en general y sensibles en particular. Específicamente, en el caso de big data, estos principios cobran relevancia, ya que la obtención de datos es de manera directa de grandes empresas, internet y otros medios masivos. Los usuarios de las redes y sistemas aceptan, tácita o expresamente, condiciones de navegación y de manipulación de sus datos que los hacen vulnerables en su intimidad y honor.

En este capítulo se indagará ¿Que herramientas existen en nuestro ordenamiento jurídico para proteger el derecho a la intimidad y la vulneración de datos personales? Y ¿En qué consisten los principios desarrollados en la ley 25.326?

Estudiaremos los principios de licitud, calidad, consentimiento, información, categorización entendida como manipulación de datos sensibles y de salud, seguridad, confidencialidad, cesión y transferencia internacional ya que, según la ley 25.326, son los que deben proveer el sustento para las buenas prácticas de big data en cuanto a datos personales, logrando así mantener el foco en las ventajas que esta herramienta brinda.

1. Archivos de datos. Licitud

Según el artículo 3 de la ley 25.326, los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública. Es por ello que los archivos serán lícitos cuando se encuentren debidamente inscriptos, y se observen en su manipulación y formación el cumplimiento de la ley y reglamentaciones que se dicten en consecuencia.

La ley define a los archivos, registro, base o banco de datos como aquellos que designan a un conjunto organizado de datos personales que son objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

También se refiere en el artículo denominado “Definiciones”, al tratamiento de datos, conceptualizándolo como el conjunto de operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Según el Reglamento europeo de protección de datos personales, artículo 6, el tratamiento de los mismos solo será lícito si el interesado dio su consentimiento para el

tratamiento de sus datos personales para uno o varios fines específicos, si es necesario para la ejecución de un contrato en el que el interesado es parte, para el cumplimiento de una obligación legal aplicable al responsable del tratamiento o es necesario para proteger intereses vitales del interesado o de otra persona física, para una misión realizada en interés público o en el ejercicio de poderes públicos, o por último, el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño[7].

La diferencia entre las legislaciones argentina y europea, es que, si bien son similares los principios enumerados, el contenido de cada uno de ellos es diferente. En el caso del principio de licitud, mientras que para la ley argentina se cumple cuando la base de datos se encuentra inscripta en el Registro y se observan los principios establecidos en la ley, en su capítulo dos; el Reglamento europeo, en su artículo 6, establece de manera precisa y enumerada, las condiciones para que el tratamiento de los datos personales sea considerado lícito.

2. Calidad de los datos

El artículo 4 de la ley 25.326 establece que los datos deben ser ciertos, adecuados, pertinentes y no excesivos, en relación con el ámbito y finalidad para los que se hubieren obtenido. En el entorno de big data, es difícil que la acumulación, reproducción, intercambio, y beneficios aportados, tengan definida una finalidad de manera anticipada y única, puesto que quizás esa acumulación masiva, directa de internet o de redes sociales, sea una de las mayores ventajas de esta herramienta, que pretende determinar tendencias o patrones y no necesariamente la obtención de datos exactos o de gran calidad. La ley debería brindar la garantía de que dichos datos no sean relacionados con sus propietarios y que, si lo hacen, cumplan con los principios establecidos en el capítulo dos de dicha ley.

La posibilidad de aportar soluciones creativas que faciliten la vida diaria de las personas, sus operaciones bancarias, vacaciones, relaciones familiares, búsquedas de ofertas, entre otras, es uno de los mayores beneficios del big data, a través del mismo

[7] Artículo 6. (Licitud). Reglamento Europeo de protección de datos personales. "El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: …"

podría estar diseñándose una solución actual con datos recolectados a través de años anteriores donde la finalidad aún era desconocida o diferente.

En cuanto a la recolección de datos no puede hacerse de forma desleal o fraudulenta, pero lo cierto es que la forma de recabar datos desde la web, internet, aplicaciones y otros softwares es cada vez más transparente y parecería que con agregar una consulta al acceder al registro con nuestros datos en las páginas ya se cubriría la solicitud realizada desde la ley, cuando los usuarios pocas veces leen las políticas de privacidad y protección de cada página.

La ley exige que se tenga conocimiento de los datos personales por cada uno de sus titulares, que se les brinde acceso y, en caso que se encuentren inexactos o incompletos, dicho titular puede solicitar su corrección, completamiento y hasta supresión por parte del responsable del archivo o base de datos (Palazzi, 2004).

También, en este artículo, se menciona que los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. Esto es casi imposible, porque el big data relaciona, genera valor actual o futuro, establece combinaciones, correlatividades entre bases, actividades, personas; en todo caso deberá buscarse la anonimización, es decir la disociación de dichos datos con los de su propietario, ya que su eliminación sería muy cara a la persona. Solamente se podrán realizar actividades de depuración basadas más en necesidades de los propietarios de las bases que en los plazos de conservación, generando archivos históricos (Gandolla, 2015).

En este sentido es pertinente aclarar que los datos obtenidos forman parte de la historia personal de cada titular, por lo tanto, su eliminación sería más perjudicial que su mantenimiento. Es fundamental su protección desde el punto de vista de la exposición pública, familiar, laboral, entre otras, pero, si consideramos que los datos pasados constituyen, por ejemplo, la historia clínica de un paciente, o la base para el cálculo de la antigüedad, o la estructura de órdenes y grados sucesorios, podemos fácilmente determinar el daño que causaría su eliminación (Palazzi, 2008). Principalmente, y siguiendo el análisis realizado por Herrera, Caramelo y Picasso (2015), a través de la ley, el estado debería establecer una función preventiva ante la publicación de datos personales o de un tratamiento no adecuado a la finalidad, una función resarcitoria si la exposición causara daños y una sanción que podría ser una rectificación pública o pecuniaria, si la exposición de dichos datos, causaran un perjuicio a su titular.

3. Consentimiento

Este principio, contenido en el artículo 5 de la ley en estudio, sostiene que el consentimiento prestado por el titular, para el tratamiento de sus datos, debe ser libre, expreso e informado, de lo contrario será ilícito.

El hecho de que sea libre, a decir de Herrera, Caramelo y Picasso (2015), se vincula con que debe tratarse de un acto voluntario, realizado con discernimiento, libertad e intención, es decir debe cumplir con el artículo 260 del Código Civil y Comercial de la Nación, mientras que el carácter de informado, hace referencia a una carga para una parte de la relación a la que la ley le adjudica el deber de suministrar información cierta y completa a la otra.

También expresa que no será necesario el consentimiento cuando los datos se obtengan de fuentes de acceso público irrestricto[8], se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, siendo que en la actualidad el estado es el responsable de una gigantesca cantidad de datos de las personas en todos los órdenes (salud, educación, trabajo, economía, hábitos, ingresos y egresos del país, familia, entre otras).

Tampoco se requiere el consentimiento cuando se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio, ya que pertenecen a fuentes de acceso público irrestricto, pero sí se mantiene la facultad del titular de solicitar la modificación, corrección o completitud si correspondiere (Palazzi,2004)

Si la relación contractual, científica o profesional del titular de los datos requiere de la manipulación de los mismos y resultan necesarios para su desarrollo o cumplimiento no se requiere el consentimiento.

Por último, tampoco lo hace, cuando 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 de entidades financieras.

El artículo 55 del Código Civil y Comercial de la Nación, afirma en cuanto a la disposición de los derechos personalísimos, que el consentimiento no se presume, es de interpretación restrictiva y libremente revocable.

[8] Artículo 3. Inciso i) Ley CABA 1845/06. Fuentes de Acceso Público Irrestricto: "… se entienden por tales a los boletines, diarios o repertorios oficiales, los medios de comunicación escritos, las guías telefónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo."

La exigencia del consentimiento expreso, no necesariamente escrito, del titular para autorizar la utilización de sus datos o imagen, no permitiéndose presumirla y estableciéndose una interpretación restrictiva, le garantiza a dicho titular su intervención ante cualquier intromisión en su intimidad. Al ser de interpretación restringida evita suposiciones de los responsables y exige, indubitablemente, el consentimiento, en caso de duda no existe tal consentimiento.

La revocabilidad como otra característica del consentimiento y permite al titular de los datos revocar la autorización previa en cualquier momento, de manera no retroactiva, con la condición que no afecte a terceros.

El doctor Ferreyra, al realizar el análisis inicial del proyecto de ley de protección de datos personales, explica el principio in dubio pro titular del dato, y resalta la asimetría existente en cuanto a poder y conocimiento entre el titular y el responsable o encargado, ya que estos últimos pueden ser el estado, grupos económicos, empresas entre otros (2018).

Es por ello que el consentimiento debe ser cierto, expreso e informado, y considerando la falta de conciencia y conocimiento de datos personales, en caso de duda entender que no hay consentimiento. Por otra parte, destaca que otra de las dificultades al momento de evaluar el consentimiento es la ambigüedad de términos tales como incompatibles, esfuerzo razonable, o como en el artículo 12 se sostiene que la forma del consentimiento dependerá de, entre otros factores, las expectativas razonables del titular del dato.

En coincidencia con este autor, se cree que se debería establecer expresamente el principio "…in dubio pro titular del dato como fórmula interpretativa que permita resolver aquellos casos en los cuales existan dudas sobre el alcance de un concepto o una excepción…" (Ferreyra, 2018, p. 3)

4. Información

El consentimiento prestado debe ser realizado previa notificación de la información del artículo 6 de la ley.

Este artículo establece que el titular del dato debe recibir información referida a la finalidad para la que serán tratados y quiénes son los destinatarios, qué archivos, bancos de datos ya sean electrónicos o de otro tipo, existen, y la identidad y domicilio del responsable.

También deberá informársele el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, y las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos.

El titular debe conocer la posibilidad de ejercer los derechos de acceso, rectificación y supresión de los datos (Palazzi, 2004).

Si no existe esta información previa, el consentimiento otorgado no será informado, por lo que resultará viciado e inválido, impidiendo realizar el tratamiento de datos o habilitando la posibilidad de recurrir a la acción de hábeas data.

El Reglamento europeo define en el Artículo 6, inciso 10, al consentimiento como la manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta el tratamiento de los datos que le conciernen de manera expresa mediante una declaración o tácitamente mediante una acción afirmativa.

El big data es llevado a cabo por empresas e inclusive por el Estado con información recabada, procesada y almacenada hace mucho tiempo, inclusive antes de la reforma de la Constitución, de la ley 25.326 y de la modificación del Código Civil y Comercial de la Nación, razón por la cual sería complejo obtener el consentimiento expreso e informado de sus titulares para su utilización, por lo que los responsables de los datos y su tratamiento, deberían extremar los cuidados.

Los responsables de los datos son definidos por la ley 25.326, como toda persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. En el proyecto de reforma de la ley se define también a los encargados del tratamiento de dichos datos como aquella persona humana o jurídica, pública o privada, que trate datos personales por cuenta del responsable del tratamiento. De esta forma separa la obtención y almacenamiento de la manipulación y transformación de los mismos.

En muchos casos, no se trata de una de falta de previsión al momento de recabar la información, sino de una falta de visión de futuro, al que, los avances tecnológicos se van encargando de hacerlo más sorprendente (Gandolla, 2015).

La creatividad al momento de buscar soluciones a problemas cotidianos, como hablar por teléfono pasando fotos, imágenes e intercambiando archivos; o de realizar compras seguras sin salir del hogar utilizando variadas formas de pago, envío y comunicación, el intercambio de procedimientos médicos, por mencionar algunos, hacen que los avances tecnológicos superen rápidamente las previsiones oportunamente consideradas por la legislación y requieran una actualización permanente.

5. Categorías de datos. Datos relativos a la salud

En los artículos 7 y 8 se enuncian dos grupos de datos que son especialmente tratados en la ley. El primero hace referencia a los datos sensibles y, según el artículo 2, determina que ninguna persona puede ser obligada a proporcionarlos, también indica que sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley o sean tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. El big data tiene recursos informáticos para llevar a cabo esa tarea a través de procesos de anonimización, en la ley 25346 se denomina disociación[9] y se describirá más adelante. Mediante la anonimización se eliminan aquellos datos susceptibles de identificar directa o indirectamente a personas concretas, manteniéndose solo información empresarial que no afecta a la privacidad personal y que puede ser usada a la hora de hacer estadísticas, análisis e investigaciones o, en el caso de big data, se utiliza para establecer tendencias y patrones.

En el inciso 3 se prohíbe, la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles exceptuando a la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales permitiéndoles llevar un registro de sus miembros.

Por último, 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. También pueden aplicarse técnicas de big data para prevención, armado de mapas de delitos, tendencias, presupuestos, entre otros, con el cuidado de proteger la identidad de los titulares a través de técnicas informáticas.

El artículo 8 establece que, respetando el secreto profesional, las entidades sanitarias públicas o privadas y los relacionados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento.

Una de las áreas más beneficiadas con los avances tecnológicos es la salud, en el caso especial de big data, permite establecer características de enfermedades, curas, tratamiento, conocimiento compartido con otros profesionales y organizaciones alrededor

[9] Artículo 2 (Definiciones) Ley 25.326 "… Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable"

del mundo, realizar interconsultas a través de internet, es por ello que extremando los cuidados de la identidad del titular es aceptable su uso.

El Reglamento europeo, en su artículo 4, inciso 5, establece el proceso de seudonimización, a fin de que el titular de los datos no pueda ser identificado. El proceso consiste en separar los datos en archivos secundarios, de manera tal que estén sujetos a medidas técnicas y organizativas que garanticen que los datos no se atribuyan a una persona física identificada o identificable.

Siguiendo el análisis realizado por (Herrera, Caramelo y Picasso, 2015) el consentimiento brindado para la realización de actos médicos e investigaciones en salud es receptado en el nuevo Código Civil y Comercial de la Nación, entendiéndoselo como la declaración de voluntad del paciente expresada a posteriori de conocer de manera clara, precisa y adecuada, los tratamientos y procedimientos a los que se expondrá, su estado de salud, los beneficios y riesgos o consecuencias adversas esperados y las posibilidades esperadas de no realizar el procedimiento propuesto. Asimismo, el decreto 1558/01, dispone, en su artículo 5, que el consentimiento informado debe ser brindado con el conocimiento del titular, precedido de una explicación adecuada a su nivel social y cultural de la información a que se refiere el artículo 6 de la ley 25.326

6. Seguridad de los datos y deber de confidencialidad

El artículo 9 obliga a los responsables[10] a adoptar medidas para garantizar la seguridad y confiabilidad de los datos almacenados, ya sean técnicas o administrativas, de modo de evitar su adulteración, pérdida, consulta o uso no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

En el artículo 10, deber de confidencialidad, se obliga a los responsables y otras personas o usuarios[11] que intervengan en el tratamiento de datos personales a mantener el secreto profesional, incluso habiendo finalizado su relación con el titular, solamente podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

[10] Artículo 2 (Definiciones) Ley 25.326 "…Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos…"

[11] Artículo 2 (Definiciones) Ley 25.326 "…Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos".

El Reglamento europeo agrega el principio de responsabilidad proactiva, en su artículo 5, por el cual los responsables de tratamiento de datos no solo tendrán que dar cumplimiento a todos los principios enumerados, sino que además deberán ser capaces de demostrar tal cumplimiento.

Es por ello que las políticas de seguridad y confidencialidad deben ser conocidas por todo el personal a cargo de los procesos de big data denominados extracción, transformación y carga (ETL por sus siglas en inglés), de manipulación, de emisión de reportes, de generación de estadísticas y pasar por exhaustivos controles de anonimización antes de ser publicados o expuestos.

7. Cesión

El artículo 11 menciona que los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.

El consentimiento es revocable y no se exige cuando es dispuesto por una ley, lo realicen los órganos del estado en cumplimiento de sus respectivas competencias, tenga fundamento en la salud pública, emergencia, epidemias y se realicen los mecanismos de disociación adecuados evitando que los titulares de los datos sean identificables.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, y éste responderá solidaria y conjuntamente por la inobservancia de las mismas ante el organismo de control y el titular de los datos de que se trate. También deberá brindar seguridad y confidencialidad a fin de evitar la adulteración de los archivos o usos no autorizados, y desvíos intencionales o no, que provengan del medio utilizado o de la acción humana (Herrera, Caramelo y Picasso, 2015).

En la causa “Torres Abad, Carmen c/ EN-JGM s/ Habeas Data”, la actora, a fin de preservar la confidencialidad de los datos brindados a la ANSES, promovió acción de hábeas data porque se utilizaron su número telefónico y correo electrónico para una finalidad distinta a la inicial, y, como estos datos no pertenecen a fuentes de acceso irrestricto, debieron solicitar el consentimiento de su titular previo a cederlos y utilizarlos con una finalidad diferente para la que fue otorgado.

La Cámara sostuvo que las excepciones del Artículo 5 deben interpretarse restrictivamente, y en cualquier otro caso se debe contar con el consentimiento expreso del titular[12].

8. Transferencia internacional

Este principio, establecido en el artículo 12, prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados, es decir que dispongan de leyes o adhesión a tratados internacionales que protejan la intimidad y los datos personales.

Establece también algunas excepciones como la colaboración judicial internacional, datos médicos por exigencia del tratamiento o investigación epidemiológica, cooperación internacional para la lucha contra el crimen organizado, el terrorismo y el narcotráfico, y transferencias bancarias o bursátiles. El flujo transnacional de datos personales es un fenómeno complejo,

> […] dicho flujo puede afectar a las condiciones de la competencia en el mercado; puede constituir en sí mismo una violación de la intimidad de las personas; puede ser necesario a los fines de un adecuado auxilio judicial o de cumplimiento de normas convencionales; puede afectar a la investigación en sectores específicos, como el sector médico respecto de los datos de los pacientes[; y] puede, finalmente, posibilitar en buen número de ocasiones, el nacimiento de supuestos de responsabilidad ex delito en [derecho internacional privado] (Oyarzábal, 2007, p. 59).

En ese sentido, la transferencia internacional de datos personales, cuando no haya una excepción de las mencionadas en la ley, procederá siempre y cuando el país receptor cuente con principios que abarquen las obligaciones y derechos de las partes y de los datos, así como un procedimiento de protección de datos que involucre mecanismos y autoridades que efectivicen la salvaguarda de la información.

Ferreyra (2018) realiza dos observaciones de casos especiales a considerar en cuanto a trasferencia internacional de datos personales. En primer lugar, analiza cuando Argentina sea parte de un tratado, y resalta las presiones por flexibilizar el flujo de datos del comercio electrónico, ya que para este tipo de negocios los datos constituyen el sustento sobre la cual las empresas tecnológicas estructuran sus negocios. La

[12] C.C.A.F. Sala V. "Torres Abad, Carmen c/EN-JGM s/ Hábeas Data" (2018)

Organización Mundial de Comercio está en la tarea de establecer estándares a fin de lograr un intercambio seguro de los datos.

En segundo lugar, estudia cuando la transferencia se realiza a una sociedad del mismo grupo económico del responsable del tratamiento evadiendo el consentimiento del titular o que el país receptor cuente con la garantía exigida.

Conclusiones Parciales

La ley 25.326 exige que los datos personales que se recaban sean exactos, y como consecuencia de ello, establece herramientas para que, en caso que fuese necesario, reclamar la supresión, sustitución o integración de los mismos. Los principios a cumplir en cuanto al tratamiento de los datos personales se encuentran entre los artículos 3 hasta el 12 inclusive, de la mencionada ley.

En el gran volumen de información recolectada, seguramente existan datos inexactos, pero, considerados y analizados en su totalidad, se obtiene un resultado más preciso y una mejor tasa de retorno que con los análisis tradicionales. Ello, por lo tanto, termina beneficiando objetivamente al individuo y dando un resultado más preciso.

Situándonos en la problemática de la incompatibilidad con los principios de protección de datos personales, vale la pena imaginar cómo se desarrollaría el ejercicio del derecho de acceso por parte de un individuo que se sienta perjudicado por la negativa a acceder a un dato que lo perjudica.

Con las nuevas técnicas de big data, se podrían establecer por cada persona, parámetros como la cantidad de amigos, o si dichos amigos tienen deudas, viajes, gustos, por ejemplo, pero si dicha información brinda una valoración negativa, no sería tan simple explicar la causa de una mala reputación.

El derecho de acceso que tiene el individuo, debería permitirle acceder a esa información y, a partir de ello, si fuera necesario, fundar un reclamo de supresión, modificación o adición, a fin de lograr la protección de su intimidad y la de sus datos personales, acudiendo a la acción de hábeas data.

Capítulo III
El big data

Prefacio

Big data es una herramienta tecnológica que facilita y posibilita tareas que, con las tecnologías existentes hasta su aparición, no podían desarrollarse, sobre todo aquellas que manipulan grandes volúmenes de información y requieren su análisis y respuesta a altas velocidades, o en períodos de tiempo muy cortos. Pero ¿De qué se trata exactamente?, ¿Cómo podemos aprovechar todo su potencial? Y, sobre todo, ¿Qué principios de protección se ponen en juego ante cada actividad de big data? Y ¿Cómo debemos protegernos de las amenazas a la privacidad y a la seguridad que trae aparejadas? (Humby, 2006).

En este capítulo se realizará la descripción del big data, brindando algunos conceptos de autores reconocidos en la materia, su caracterización a través de las cinco V establecidas por Humbry, en 2006, y la relación de sus actividades y procedimientos en cuanto a datos personales y derecho a la intimidad se refieren.

El big data no solo manipula datos estructurados, la exposición de sonidos, imágenes, películas, planos, mapas, a través de datos no estructurados, hacen más amplio el campo personal expuesto y en consecuencia mayor la tarea de protección.

1. Caracterización del big data. Concepto

Una herramienta que inició su desarrollo a principios del siglo XXI y avanza exponencialmente en la actualidad, es el big data, definido por el Oxford English Dictionary, como el conjunto de datos extremadamente grandes que deben ser analizados computacionalmente para revelar patrones, tendencias y asociaciones, especialmente relacionadas al comportamiento humano y a las interacciones y cuyo mayor valor surge de la capacidad para producir conocimiento y comunicarlo de manera eficiente, fácilmente comprensible, accionable y escalable en beneficio de la comunidad (Oxford University, 2013).

Aunque no hay una definición única para este fenómeno, la opción planteada por el informático norteamericano John Mashey, es una de las más utilizadas. Define al big data como un término que se aplica a sets de datos, cuyo tamaño está más allá de lo que las herramientas de software habitualmente utilizadas pueden capturar, administrar y procesar, en un período de tiempo razonable (Mashey, 1998).

Las herramientas habituales a las que se refiere, son los administradores de bases de datos, software de aplicación, planillas, generadores de aplicaciones y cualquier otro instrumento de manipulación de datos tradicional, que se diferencian de los de big data

puesto que estos últimos contienen desarrollos específicos para las etapas denominadas ETL , extracción, transformación y carga, permitiendo manejar volúmenes variados y crecientes de datos medidos en terabytes, petabytes, exabytes y más, a gran velocidad. La especificación de tiempo razonable, se relaciona con la utilidad y oportunidad de los datos. Si se producen tempranamente pero no se define su uso u objetivo, sería un dato irrelevante, por otra parte, si se lo obtiene o procesa tardíamente puede que ya sea obsoleto.

El big data, según De Ángelis (2016), basa su rápida expansión en el crecimiento exponencial, la producción y el almacenamiento incesantes de grandes volúmenes de datos, y en el desarrollo de gran capacidad para analizar, comprender y aprovechar el valor de esos datos. Estas actividades también alcanzan a las ciencias sociales donde esos flujos de datos, en grandes volúmenes y a altas velocidades provenientes en gran proporción desde Internet, enfrentan a los científicos sociales a nuevos desafíos.

2. Las cinco dimensiones del big data

Existe un amplio consenso en torno a las tres características que lo definieron inicialmente, denominadas tres V (velocidad, variedad, volumen) a las que se agregan veracidad y valor, conformando las cinco V del big data. La tecnología permite que las personas estén hoy ultra conectadas; esta interconexión genera una cantidad de información nunca antes vista (Humby, 2006).

2.1. Velocidad

La velocidad con que los datos son creados o generados ha aumentado de forma considerable, requiriendo una respuesta adecuada para su procesamiento y análisis. Esta velocidad de respuesta es necesaria para hacer frente a la obsolescencia de los datos debido a su rápida capacidad de generación, haciendo poco útil lo que instantes antes era válido; de ahí que el procesamiento distribuido y paralelo sea una de las tecnologías que soporten el concepto de big data.

Por otra parte, la necesidad de que un analista de datos sepa identificar, para cada aplicación, los datos cuyo ciclo de vida sea muy corto de los que tienen un ciclo de vida mayor, se determina como fundamental a la hora de rentabilizar y optimizar los usos adecuados de los recursos, aumentando la precisión y calidad de los resultados.

Esta situación trae como consecuencia, definir el tratamiento que deben dar los responsables de las bases de datos, a estos datos tan cambiantes y tan velozmente

producidos, una vez que ya cumplieron con la finalidad por la que fueron colectados. Deben decidir si se archivan, se dan de baja, se actualizan, se los mantiene indefinidamente o se aplica el derecho al olvido que el Reglamento europeo de protección de datos personales, tiene definido y que funciona a pleno. En nuestro país, éste último punto, derecho al olvido, fue rechazado por la Corte Suprema de Justicia en la causa Gimbutas[13] al negar la responsabilidad a los buscadores de internet.

Los datos son almacenados en diferentes medios, no sólo propios, sino en espacios gratuitos o pagos provistos en las redes. No todos estos espacios de guardado tienen las mismas normas de seguridad, pero al disponer de espacio prácticamente ilimitado y a bajo costo, las empresas, e incluso los particulares, no analizan estrictamente la función y uso que darán a los datos, sino que los guardan para ver si los pueden aprovechar a futuro.

2.2. Variedad

La variedad en big data se basa en la diversidad de los tipos de datos y de las diferentes fuentes de obtención de los mismos. Así, los tipos de datos, podrán ser estructurados, desestructurados o semiestructurados.

Los primeros son los que tienen bien definidos su longitud y su formato, como las fechas, los números o las cadenas de caracteres. Generalmente están almacenados en tablas. Como ejemplo están las hojas de cálculo o las bases de datos.

Los desestructurados son los que se encuentran en el formato tal y como fueron recolectados, carecen de un formato específico. No se pueden almacenar dentro de una tabla ya que no se puede desgranar su información a tipos básicos de datos. Como ejemplo son los documentos de texto, las películas, los correos electrónicos o los archivos PDF.

Los semiestructurados no se limitan a campos determinados, sino que contienen marcadores para separar los diferentes elementos. Es una información poco regular como para ser gestionada de una forma estándar. Estos datos poseen sus propios metadatos semiestructurados que describen los objetos y las relaciones entre ellos, y pueden acabar siendo aceptados por convención. Como ejemplo es el caso del HTML (García Barbosa, Hernández de Rojas, García Esteban, Lopez Lopez y Nuñez, 2015).

Otra clasificación, considerando las fuentes, es de acuerdo a como se generan y producen los datos (Comisión Europea, Dirección General de Redes de Comunicación, Contenido y Tecnologías, 2017).

[13] C.S.J.N., "Gimbutas, Carolina Valeria c/ Google Inc. s/hábeas data". Fallos 340:1236 (2017).

Al respecto se podría decir que, el primer grupo, es el de los datos producidos por la interacción de las personas, al enviar y responder mensajes y correos, realizar publicaciones y reacciones en las redes sociales, por la utilización de motores de búsquedas o en la generación de todo tipo de documentos.

Las transacciones producen datos, mediante las diferentes operaciones entre cuentas, clientes, sucursales, las llamadas o los procesos automáticos de particulares y empresas. Las transacciones bancarias son un ejemplo claro al respecto. Este es el segundo grupo de datos automáticos.

El marketing en línea, el comercio electrónico y en la red, producido al navegar por internet, conforman el tercer grupo, donde se genera una gran cantidad de datos, no solo a nivel de las páginas de visita, sino a nivel de tiempo de permanencia en cada una, cuáles fueron los contenidos de mayor interés, y cuándo y cuántas veces visita una persona dichas páginas.

Otros datos se producen entre máquinas y hacen referencia a aquellas tecnologías que comparten datos con todo tipo de dispositivos, como pueden ser los medidores, los sensores, geo-localizadores; como ejemplo se encuentran los termómetros marinos, sensores eólicos o sísmicos, GPS.

La biométrica produce un conjunto de datos que provienen o están relacionados con la seguridad, defensa y servicios de inteligencia. Son generados por dispositivos como los lectores biométricos, lectores de huella de retina y demás. En nuestro ordenamiento jurídico, los datos biométricos no son considerados sensibles, como sí lo son según el reglamento de protección de datos personales de la Unión Europea (Reglamento europeo, 2018). No obstante, se utilizan en operaciones de extrema seguridad como los cajeros automáticos y para control a áreas restringidas, tendiéndose a que la identificación personal se realice por estos medios, a fin de evitar gran cantidad de usuarios y contraseñas que dificultan enormemente su mantenimiento y las operaciones a los usuarios.

Es decir, los datos provienen de una diversidad de fuentes y almacenamientos como archivos de textos e imágenes, la web, redes sociales, sensores dispuestos en las fábricas, ciudades, aeropuertos, entre otros. Esta variedad determina la riqueza, que, en sí, conlleva el concepto de big data. Sin embargo, esta potencial riqueza aumenta el grado de complejidad, tanto en su almacenamiento como en su procesamiento y análisis.

En lo referido estrictamente a datos personales es necesario diferenciar los definidos en la ley 25.326 como sensibles y de salud, a fin de realizar una protección mayor en su manipulación y exposición.

2.3 Volumen

La dimensión de volumen, es quizás, la característica más asociada al concepto de big data. Las estimaciones de aumento de datos generados indican un crecimiento sin precedentes, debido a las redes sociales y a la movilidad que facilitan las redes inalámbricas y la telefonía móvil. Este incremento de datos determina un cambio de escala pasando de terabytes a petabytes, exabytes y zetabytes de información, dificultando su manipulación. Sin embargo, mucha de esta información, según el tipo de utilización, puede pasar a tener un ciclo de vida de su valor muy corto, convirtiéndose en obsoleta de forma muy rápida. Este tipo de apreciación se enlaza con la dimensión de velocidad.

En big data la gran cantidad de datos que se recolectan y analizan gracias a las nuevas técnicas, casi por definición o con gran pérdida de valor, contendrán información errónea o con una vida muy corta (Gandolla, 2015).

Un ejemplo de lo planteado lo encontramos en las empresas que han comenzado a analizar la solvencia financiera de las personas a partir, no ya de su patrimonio o de sus antecedentes con la entidad, sino de la información recolectada en diversos medios, como redes sociales. Así, por ejemplo, el estado social para crédito, considera la reputación y el estatus social online y los contactos como factores fundamentales, en particular, para solicitantes con poco historial crediticio.

La ley de protección de datos personales, en su artículo 20, prohíbe tal práctica como única herramienta para tomar una decisión de aceptación o rechazo de una solicitud. Además, la ley 21.526, de entidades financieras, en su artículo 39, norma que dichas entidades no podrán revelar las operaciones pasivas que realicen, brindando así seguridad y privacidad al titular.

No obstante esta restricción, la disponibilidad de grandes volúmenes de datos sobre operaciones financieras realizadas por los clientes u obtenidas a través de recursos de páginas web como Google por un lado, y el uso de técnicas como el big data por el otro, permite a dichas entidades financieras establecer tendencias, identificar patrones y diseñar aplicaciones inteligentes, emprender campañas, ofrecer productos personalizados de manera más segura y sin arriesgar la protección de los datos de sus clientes.

2.4 Veracidad

Una de las características asociada a la calidad de los datos es la veracidad de los mismos. La veracidad puede entenderse como el grado de confianza que se establece sobre los datos a utilizar. Dentro de la caracterización del big data, la veracidad determina su cuarta dimensión, y es de gran importancia para un analista de datos, ya que es la que definirá la calidad de los resultados y la confianza en los mismos (Humby, 2006).

Por lo tanto, un alto volumen de información que crece a velocidad muy rápida y basada en diferentes tipos de datos provenientes de una gran variedad fuentes, hacen inevitable dudar del grado de veracidad de los mismos. Por ello, dependiendo de la aplicación que se les dé, su veracidad puede ser imprescindible o convertirse en un acto de confianza sin llegar a ser vital (Doan, Halevy & Ives, 2012).

Es necesario invertir tiempo en el análisis y transformación previos a la carga de datos para conseguir que éstos sean de calidad, reduciendo o eliminando datos imprevisibles o no válidos, disminuyendo así el nivel de incertidumbre.

2.5 Valor

Desde el punto de vista de la recolección y explotación, la dimensión valor representa el aspecto más relevante del big data. Actualmente en cuanto al valor marginal de los datos se observa que a medida que aumenta el volumen y complejidad de los datos, su valor marginal disminuye considerablemente, debido a su dificultad de explotación (Laboratorio de Big Data, 2014).

Aumentar el valor marginal de los datos es uno de los retos actuales desde el punto de vista de la tecnología, del analista, y finalmente del gestor en la mejora de la toma de decisiones, de una forma rápida, inmediata y precisa. Esto será útil para establecer tendencias, proyectar mejoras, optimizar los aspectos competitivos de ciertas áreas, entre otras (Laboratorio de Big Data, 2014).

Facilitar la explotación de los datos para obtención de valor, sigue siendo el objetivo fundamental de la inteligencia de negocios y, ahora, de las tecnologías del big data (De Ángelis, 2016). Sus aplicaciones son tan amplias y variadas que abarcan desde el diseño de estructuras de big data para establecer tendencias financieras y de mercados, hasta la posibilidad de usar sus aportes para reclutar equipos deportivos, estudiar enfermedades, analizar el cambio climático, y en todos los casos su gran fortaleza es la capacidad para establecer tendencias y patrones.

3. Ventajas del uso del big data para la sociedad.

Big data es el resultado de lo que se produce en el ámbito empresarial y administrativo, en las redes sociales y en internet. La Comisión Económica de las Naciones Unidas para Europa, UNECE, por sus siglas en inglés, también incluye dentro de este concepto, lo generado por los motores de búsqueda en internet y por dispositivos móviles.

Como lo señala Gandolla (2015), hay quienes consideran que el tratamiento de datos llevado adelante mediante el big data puede ser tan beneficioso para la sociedad, como peligroso para la privacidad de las personas y, por lo tanto, se deberán poner límites y encontrar una solución equilibrada.

Big data, el vocablo de moda, cada vez más presente en el discurso de consultores, empresarios, políticos y hasta deportistas, ofrece un conjunto de posibilidades hasta ahora inimaginables, aunque hasta a los expertos les resulta difícil terminar de dimensionar este fenómeno y sus consecuencias.

De acuerdo a la división de Naciones Unidas, denominada UN Global Pulse, cuyo objetivo es acelerar el descubrimiento, el desarrollo y la adopción a escala de big data, para el desarrollo sustentable e iniciativas humanitarias, la humanidad se encuentra en medio de una revolución industrial de los datos, término acuñado por el científico informático, Joe Hellerstein en 2012, que se caracteriza por un incremento exponencial en la cantidad y diversidad de datos digitales disponibles en tiempo real, producto de un mayor uso de equipos tecnológicos con más capacidad en la vida diaria, lo que permite obtener un profundo conocimiento del comportamiento humano (Doan, Halevy, Ives,2012).

Las finalidades perseguidas por un proyecto big data pueden ser muy variadas. Los de inteligencia comercial, engloban a todos aquellos proyectos big data que persiguen un conocimiento profundo y predictivo de los clientes que interactúan con el propietario o impulsor del proyecto.

Estos proyectos buscan mejorar la experiencia del cliente en su relación con la empresa, prevenir y evitar que se corte la relación con el negocio, generar patrones de comportamiento y segmentaciones avanzadas de clientes o la oferta personalizada de productos, servicios y precios, prevención de fraude y riesgo consistentes en la previsión y predicción de posibles actividades fraudulentas que redunden en perjuicio del impulsor

del proyecto, desde las de sus propios clientes y proveedores, hasta de otros elementos externos como la ciberseguridad o la prevención de fallos de sistemas. Los proyectos de big data buscan maximizar la eficiencia operativa en objetivos encaminados a optimizar los procesos productivos o de toma de decisiones, incluyendo proyectos asociados al internet de las cosas, eficiencia en la gestión logística y de flotas, o de optimización en la gestión de reclamos y devoluciones.

También están los proyectos big data que persiguen un beneficio económico directo, a través de la generación de nuevos negocios en entorno digital, aplicaciones para celulares, empresas tecnológicas, intermediación en comercio electrónico, entre otros.

Incluso se está desarrollando esta tecnología para usos tales, como el estudio de enfermedades, epidemias, reclutar jugadores para una actividad deportiva, aumentar el rendimiento de los soldados en el campo, mejorar las técnicas de determinadas profesiones, entre otras.

Al estudiar estos datos, los científicos pueden crear distintos perfiles en función del comportamiento de los usuarios. Dichos perfiles, analizados en el tiempo, crean patrones que permiten elaborar predicciones de futuro, tendencias con las que se hacen recomendaciones personalizadas a los clientes para ayudarlos en su vida cotidiana, y brindar soporte para la toma de decisiones organizacionales.

4. Riesgos o inconvenientes de su aplicación

Las redes sociales, junto a la facilidad e inmediatez de las redes inalámbricas y la telefonía móvil, los nuevos servicios de almacenamiento en la nube, entre otros, han propiciado, que cada vez se genere un mayor volumen de datos, y de forma muy rápida, provenientes de diferentes fuentes de información, cuya veracidad es difícil de constatar, así como su consentimiento informado, que a veces, es inexistente, y cuyo tiempo de validez puede no ser muy grande. Con este tipo de escenarios, relevados por la experiencia de las empresas basadas en internet, uno de los retos actuales de la implantación de la tecnología asociada al concepto de big data, es llegar a verlos, no como una dificultad, sino como una ventaja competitiva, poniendo el mayor esfuerzo en cumplir con los principios del ordenamiento jurídico.

Ante esta situación la ley 25.326, en su artículo 23, trata algunos supuestos especiales tales como los datos personales que, por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos, y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las

autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

Los datos personales registrados con fines policiales, según la ley de protección de datos personales, se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

4.1 Origen de los datos

En cuanto al origen y obtención de los datos hay aspectos jurídicos principalmente de privacidad, intimidad y protección de datos personales que requieren no solo la determinación de la finalidad de su registro, sino también como son producidos, quién los genera y con qué autorización. Como se mencionara en el capítulo uno de este trabajo, es indiscutible que éstos son aspectos fundamentales que deben considerarse a la hora de analizar los proyectos big data desde un punto de vista jurídico.

En el momento de recabar sus datos gran parte de los proyectos big data, corre el riesgo de incumplir con la salvaguarda para la privacidad personal, bien porque la combinación de los datos ya disponibles con nuevas fuentes de datos adicionales permite generar perfiles personales sin que exista consentimiento previo para ello, bien porque los objetivos del proyecto conducen a usos de datos que no eran razonablemente previsibles para los interesados en el momento inicial de obtención de sus datos. Para superar estas situaciones de riesgo, las autoridades europeas en materia de protección de datos recomiendan someter el proyecto big data a un test de incompatibilidad. En la Argentina aún no se cuenta con procesos de este tipo, pero las empresas que hacen big data comienzan a orientar sus proyectos a mejorar el tratamiento no solo del punto de vista de la eficiencia, sino también de la ley.

Según Eduardo Peduto, Director del Centro de protección de datos personales de la ciudad de Buenos Aires en el año 2014, uno de los mayores desafíos que plantea el uso

de big data se basa en que, si bien las posibilidades comerciales y financieras que abre el big data son enormes, desde su punto de vista, la cuestión más importante está dada por la configuración de los perfiles sociales. Esto tiene que ver con el modo en que se puede inclinar la opinión pública, no sólo a partir de gustos y preferencias, sino también a partir de miedos y presiones. Otro tema asociado, que es la falsa ilusión que se creó en su momento respecto del desarrollo de Internet: la supuesta democratización de la información. En realidad, según Peduto, hoy tenemos un círculo muy pequeño que orienta la opinión pública.

También advierte que "una gran falencia que nos excede como país es la inaplicabilidad de nuestra legislación nacional frente a los grandes monstruos de Internet" (Peduto, 2014). Los contratos de adhesión a Google o a Facebook establecen que, ante cualquier litigio, los tribunales competentes son los de California.

El hecho de que el hábeas data se encuentre contemplado en nuestra Constitución Nacional nos da cierta fortaleza. Sin embargo, tenemos inconvenientes de tipo operativo. Cuando se sancionó la ley nacional, si bien ya existía cierto desarrollo informático, de ninguna manera había alcanzado los niveles que hoy tiene la intercomunicación internacional.

En algunos países, como España, el acceso a internet es considerado un derecho universal tanto para hombres como para mujeres, a través del cual se procurará la superación de la brecha de género, tanto en el ámbito personal como laboral, así como colaborará con la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores (Sanchez Bravo,2001).

La ley 25.326, no contempla ninguna de estas posibilidades de achicar brechas, sino que trata la protección de datos como relacionados a personas físicas, denominados titulares cuyo consentimiento es necesario, y solamente aborda supuestos de perjuicios o daños a la intimidad con su correspondiente sanción o garantía constitucional y el derecho a la información.

4.2 Transparencia

Además de proteger la privacidad también es necesario que exista transparencia para que las personas humanas posean total acceso a todos los datos que han sido recogidos sobre ellas, de esta forma podrán ejercer los derechos sobre sus datos.

También debemos tener en cuenta otros aspectos como la distribución o la venta de datos entre grupos de empresas, el robo masivo de datos producidos a distintas empresas

variadas, como entidades bancarias o redes profesionales y acciones directas de empresas y agencias de inteligencia para obtener todo tipo de datos mediante acciones de escucha o activación de cámaras en dispositivos móviles o la captura de archivos personales y empresariales. Todo esto no disminuye el grado de responsabilidad de los usuarios de distribuir sus datos personales y la utilización y actualización periódica de aplicaciones de protección tendientes a minimizar los riesgos de robo de datos personales, sino que aumenta la necesidad de protección (Humby, 2006).

Respecto a la privacidad, resulta muy importante determinar la cuestión de quién en definitiva es el dueño de los datos que se analizan. Podemos preguntarnos, por ejemplo, ¿Quién es el dueño de los datos que se recogen sobre nuestras interacciones con nuestros dispositivos móviles? ¿Pertenecen a la persona que interactúa, a la compañía que presta el servicio de acceso a Internet, a la empresa propietaria de los contenidos que visitamos o a cualquier agencia de inteligencia gubernamental que pueda acceder a ellos?

Gran parte del valor de los datos suele estar en los distintos usos indirectos que son diferentes de aquellos para los que fueron recolectados en su momento. De ello podemos concluir que puede llegar a existir un cierto riesgo de que los datos se analicen con fines distintos que los sujetos de los datos ni conocen, ni aprueban. Además de proteger la privacidad también es necesario que exista transparencia para que las personas tengan total acceso a todos los datos que han sido recogidos sobre ellas, de esta forma poder ejercer los derechos sobre dichos datos.

También debemos tener en cuenta otros aspectos, como el robo de datos a empresas (tarjetas de crédito, Facebook, etc.), los hackeos, la distribución o venta de datos entre empresas, las acciones deliberadas de empresas y agencias de inteligencia para obtener todo tipo de datos a través de cámaras de video o vigilancia, micrófonos, escuchas, dispositivos USB, para la captura de datos personales o empresariales, que de ninguna manera disminuyen la responsabilidad de los encargados del tratamiento y seguridad de los datos, pero que encienden las alertas para optimizar los controles.

Los usuarios continúan siendo, además, los responsables de distribuir sus datos personales o de consentir a su utilización y distribución, y de actualizar periódicamente las aplicaciones de protección tendientes a minimizar los riesgos de robo de datos personales, mejorar sus contraseñas, y tomar las medidas de prevención necesarias. Esto aumenta la necesidad de mejorar las formas de obtener el consentimiento y la manera de transparentar los procesos de recolección y almacenado, y sobre todo optimizar el control de las empresas que realizan los tratamientos informatizados.

4.3 Calidad y conservación. Derecho al olvido

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, introduce nuevos elementos como el derecho al olvido y el derecho a la portabilidad. Ambos derechos tienen la finalidad de mejorar el control de los ciudadanos sobre los datos personales que son confiados a terceros.

El derecho al olvido se presenta como la consecuencia del derecho que poseen los ciudadanos a solicitar, y obtener de los responsables, que sus datos personales sean suprimidos cuando ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando hayan sido recogidos o tratados de una manera no lícita.

El reglamento recoge expresamente la posibilidad de que se ejerza el derecho al olvido, este derecho ya fue reconocido por la jurisprudencia del Tribunal de Justicia de la Unión Europea desde el 13 de mayo de 2014. Los interesados pueden solicitar a las empresas responsables que sus datos personales sean suprimidos y también pueden solicitar la recuperación de sus datos, siempre que su tratamiento hubiera sido automatizado, para su posterior transmisión a otras entidades.

El titular de los datos tendrá derecho a obtener, del responsable del tratamiento, la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo, se retire el consentimiento o los datos se traten ilícitamente. La supresión puede ser derivada del cumplimento de una obligación legal, o en razón de salud pública, entre otros (Reglamento europeo, 2018).

En nuestro ordenamiento jurídico se encuentra en estudio la modificación a la ley de protección de datos personales que ya fue elevada a la Legislatura, mediante el Mensaje 147/18 del Poder Ejecutivo, donde se profundizan y se siguen los lineamientos ya desarrollados en la Unión Europea, tanto para protección interna, como para adecuación a los estándares requeridos para intercambios internacionales.

Una de las acciones que puede solicitar el titular de los datos es la supresión de los que considera que lo perjudican o no quiere que se archiven en bancos de datos privados o públicos, hasta allí podría traducirse como el derecho al olvido europeo, pero en nuestro

país la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

Además, dependiendo del tipo de datos y el medio o fuente receptora, por ejemplo, los medios de comunicación, hay riesgos de que se configure como censura, por lo que el concepto de derecho al olvido no es absoluto, sino una herramienta más, a través cual el titular podría solicitar la supresión de sus datos para defender su derecho a la intimidad.

4.4 Decisiones automatizadas

El principio de impugnación de valoraciones personales informatizadas, se desarrolla en el artículo 20 de la ley de protección de datos personales, y en él se establece que las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.

Este principio no se encuentra en el capítulo II de la ley, principios generales relativos a la protección de datos, sino en el referido a Derechos de los titulares de los datos, es decir en el capítulo III.

Independientemente de que en nuestro país se interprete que este derecho puede o no ejercerse frente a privados, debemos hacer notar que, a través del big data, en la utilización comercial de los datos que se lleva a cabo, por ejemplo, en el área de marketing, se generan permanentemente perfiles mediante los cuales se segmenta el mercado, se establecen campañas, se conocen hábitos.

Si bien la norma argentina no establece expresamente, que el titular de los datos tiene derecho de obtener información sobre los criterios de valoración y los programas utilizados, se podría entender que el derecho de acceso, en sentido amplio, brinda dicha posibilidad (Gandolla, 2015).

El titular puede oponerse cuando la decisión que lo afecte negativamente, o le produzca efectos jurídicos perjudiciales, esté basada únicamente en el tratamiento automatizado de datos, excepto que haya dado su consentimiento expreso, se encuentre autorizada por la ley, o sea necesaria para la ejecución del contrato entre el titular y el responsable del tratamiento.

Cabe aclarar que el consentimiento puede ser revocado en cualquier momento, bastando para ello una comunicación expresa, debiendo previamente verificarse que no

perjudique a terceros. La revocación no es retroactiva, es decir sus efectos serán desde el momento de su presentación hacia adelante en el tiempo.

Conclusiones Parciales

La velocidad de producción de datos y la gran valoración que adquiere el conocimiento, hacen necesario que el orden jurídico se mantenga alerta y cubra áreas que no solo no se previeron, sino que antes no existían porque era casi imposible imaginarlas: trabajos colaborativos mundialmente, inteligencia de negocios, redes sociales, comercio global, telecomunicaciones, minería de datos, redes de altísima velocidad, las nubes de almacenamiento y procesamiento, internet y tecnología al alcance de la gran mayoría, entre otras.

Se describieron las características de big data, indicando en cada una los peligros latentes en los que la exposición de datos cuenta con menor seguridad y confiabilidad, se detallaron ventajas y riesgos o inconvenientes en su aplicación, y la necesidad de constantemente evaluar los sistemas que los utilizan y cuan efectivas son sus estrategias para cumplir los principios descriptos en el capítulo II de la ley 25.326.

Se hizo hincapié en varios puntos en los que, según la ley 25.326, se requiere especial cuidado, como el origen, la transparencia, la calidad y conservación de los datos, siendo éste uno de los puntos más afectados por esta herramienta, y la posibilidad y riesgo de tomar decisiones automatizadas basadas solamente en procesos informáticos.

Las condiciones de uso de las páginas web afirman que, su recolección de datos, es con fines estadísticos, de seguridad y de personalización, pero como vemos a diario, también se utilizan para determinar los hábitos de compras, preferencias, actividades y enviar un sinfín de publicidades ofreciendo servicios relacionados. Estas actividades están sumamente relacionadas con el big data y con la consecuente falta de cumplimiento de los principios de la ley.

Las ventajas que trae esta herramienta a la sociedad en todos sus ámbitos es innegable, pero su uso debe ir aparejado con el ordenamiento jurídico para evitar lesiones a derechos constitucionales de las personas.

Capítulo IV

La acción de protección, hábeas data. Jurisprudencia

Prefacio

La acción de hábeas data se encuentra en el Capítulo VII de la ley de protección de datos personales. En este capítulo se estudiarán la procedencia, los legitimados activos y pasivos, la clasificación según Pedro Sagués, para así posteriormente caracterizar algunos casos de importantes tribunales argentinos.

Se responderá a las preguntas ¿Cuál es el objetivo de recurrir a la acción de hábeas data y su procedencia? Y ¿Cuáles son los presupuestos con los que los Tribunales nacionales, a través de sus fallos, aplican la Ley 25.326 en relación al big data?

Se tratará, en cada caso particular, de indicar con cuál de los principios de la ley se relaciona y las posibilidades legales de actuar si algunos de ellos son incumplidos y bajo qué argumentos normativos el big data entra en tensión con el derecho a la intimidad y la protección de los datos personales en los supuestos señalados.

Los principios descriptos en el capítulo II de la ley 25.326 son los de licitud, calidad, consentimiento, información, categorización entendida como manipulación de datos sensibles y de salud, seguridad, confidencialidad, cesión y transferencia internacional, a los que le podemos agregar el derecho al olvido para lograr la eliminación de la información del usuario que ha dejado de ser necesaria para el fin para el cual fue recolectada, que en el caso de las redes sociales, sólo debe limitarse a la prestación del servicio.

1. Procedencia

El Capítulo VII de la ley de protección de datos personales se destina a la acción de protección.

Se podrá recurrir a ella, según el artículo 31, para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos. Si bien es cierto que se debe prestar consentimiento informado para la obtención y manipulación de estos datos, la realidad es que ya hay datos que se encuentran en poder de empresas, organizaciones o el Estado y la ley ampara el derecho de solicitar información acerca de los mismos.

También será procedente esta acción en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. Quedan fuera del hábeas data, los archivos o registros de y para uso exclusivo de su propietario, ya que todo ello está amparado por la

intimidad y privacidad que otorga el Artículo 19 de la Constitución y por la inviolabilidad de los papeles privados, del Artículo 18 de la misma ley fundamental.

Por lo que la procedencia de la acción de protección se encuentra regulada con la más alta jerarquía dentro del ordenamiento jurídico argentino, de lo cual se hace eco la ley de protección de datos personales. Se puede decir que una vulneración a cualquiera de sus principios, otorgaría al titular el derecho de solicitar a los responsables, la eliminación, modificación o actualización en la medida que produzca lesiones a su intimidad. Esta garantía constitucional, evidencia el valor o la importancia de los datos personales para sus titulares como parte de los derechos personalísimos.

2. Legitimación

La acción de protección podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado, según la legitimación activa otorgada en el artículo 34 de la ley de protección de datos personales.

La acción procederá, según el artículo 35 de la ley 25.326, contra los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes. Aquí también se discute si sólo se puede solicitar información si estos bancos de datos brindan informes o, en cualquier caso. La tendencia jurisprudencial es considerar que todos los bancos de datos, estén o no destinados a proveer informes, deben cumplir con los recaudos de la ley 25.326 (Sistema Argentino de Información Jurídica, 2018). Los datos recolectados por big data, pocas veces producen informes personales, sino que se utilizan mayormente para establecer tendencias, pero igualmente la protección se basa sobre todo en la anonimización o efectiva disociación del dato con su propietario o titular.

3. Competencia

Según el artículo 31 de la ley 25.326, será competente el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Procederá la competencia federal cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y cuando los archivos de datos se encuentren interconectados en redes inter jurisdicciones, nacionales o internacionales.

4. Tipos de hábeas data

Según Pedro Sagués, el instituto de hábeas data admite ciertos tipos, que se explican a continuación, pero deberían tenerse en cuenta otras modalidades que pueden surgir de la experiencia jurídica, y que complementan al artículo 43 de nuestra constitución (Sagués, 2017).

La clasificación propuesta por este autor es la que se sigue en este trabajo.

4.1 Hábeas data informativo

Su objeto es recabar información obrante en registros o banco de datos públicos o privados destinados a proveer informes. Existen, según este autor, tres subespecies:

a) Hábeas data exhibitorio. Permite a una persona conocer qué se registró de ella. Su fin es el conocimiento de los datos referidos a la persona que articula al hábeas data. Se encuentra desarrollado en la ley 25.326.

El hábeas data exhibitorio simple, implica ejercitar el derecho de acceso a la base de datos, por parte del registrado. Ekmekdjian y Pizzolo se preguntan si ese derecho involucra la facultad de ingresar física y personalmente a esa base, si hay que evaluar los casos en los que esto puede realizarse para constatar la exactitud o veracidad, y si solo puede realizarse con autorización judicial o por ejemplo en un proceso de la AFIP. “De lo contrario, el éxito del hábeas data quedaría a merced del informante” (Ekmekdjian y Pizzolo,1996, p.68).

b) Hábeas data finalista. Su objeto es saber para qué y para quién se registran los datos, como ya describimos en el capítulo dos de este trabajo. Los datos se recolectan, almacenan y manipulan con una finalidad determinada que debe ser conocida por el titular de los datos. También pueden solicitarse los datos de otros responsables relacionados o entre los cuales se intercambian datos y verificar la finalidad con la que los mismos son registrados. La responsabilidad de los intervinientes es solidaria ante el titular.

c) Hábeas data autoral. Si bien es poco habitual en la doctrina y en el derecho comparado, en la actualidad la información se distribuye tan fácilmente y es objeto de intercambio y negocios, que la identificación de cada interviniente en la cadena de manipulación debería ser precisa y clara. Su objeto es conocer quien obtuvo los datos que obran en el registro y así diferenciar el productor, el exportador, el distribuidor y el manipulador. No podrá afectarse el secreto de las fuentes de información periodística, pero mediante un hábeas data, sería factible consultar sobre fuentes que no estuvieran

afectadas por secretos relacionados con defensa, seguridad, salud, o preguntar por las fuentes de información no periodística.

4.2 Hábeas data aditivo

Su propósito, previsto en el artículo 43 de la Constitución Nacional, es agregar más datos a los que constan en el respectivo banco o base de datos. El caso más común es el de poner al día información desactualizada, por ejemplo, si alguien aparece como deudor, habiendo satisfecho su obligación; o si figura como procesado, habiendo sido en definitiva sobreseído.

4.3 El hábeas data rectificador

Apunta a corregir errores en los registros almacenados en bases o bancos de datos, esto es, actualizar datos falsos o erróneos, como adicionar el apellido materno, o modificar el domicilio.

4.4 El hábeas data reservador

Su objeto es asegurar la confidencialidad de ciertos datos como parte del derecho a la intimidad, protegida por el artículo 19 de nuestra Constitución. Está contemplado en el artículo 43 y fue introducido en la reforma constitucional de 1994. En este caso, el dato es cierto y no hay obstáculos para su conservación, por parte del registro respectivo. Pero su divulgación puede causar daños por lo que se ordena al titular del registro que lo mantenga para su uso personal exclusivo, o para su empleo específico a los fines legales pertinentes. Por ejemplo, las historias laborales o clínicas.

4.5 Hábeas data cancelatorio o exclutorio

Se refiere a información sensible, potencialmente discriminatoria o lesiva del honor o la privacidad. Son los datos referidos a ideas políticas, religiosas o gremiales, al comportamiento sexual, a ciertas enfermedades o datos raciales.

Estos datos sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley o con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Por otra parte, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. En cuanto a 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.[14]

4.6 Mixto

El Hábeas Data puede ser mixto, es decir perseguir más de una de las finalidades de esta acción, puede, por ejemplo, comprender un objetivo exhibitorio y a la vez solicitar la actualización o rectificación de algunos de los datos en poder del banco de datos.

Con esta determinación de tipos se pretende abarcar todos los supuestos en que los datos almacenados y manipulados por responsables, causen un daño al titular, o avasallen su intimidad. No obstante, la tecnología y los medios de comunicación amplían sus fronteras día a día, razón por la cual no estaría de más suponer que en poco tiempo se requiera un tipo de protección más amplio y con mayor variedad.

5. Casos de fallos de la Corte Suprema de Justicia de la Nación, de la Cámara Nacional de apelaciones Civil y Comercial Federal y de otros tribunales nacionales sobre derecho a la intimidad y hábeas data.

La Corte Suprema de Justicia de la Nación, en el 2017, reafirma su doctrina en materia de responsabilidad de los buscadores de internet, encontrando su fundamento en la libertad de expresión, en la causa Gimbutas[15]. En el fallo de Rodríguez, María Belén[16], del año 2014, había dictaminado en similar forma resolviendo que la actividad de los buscadores de internet se encuentra amparada por tal libertad. La determinación del recolector y manipulador de los datos, cobra importancia en los procesos de la anonimización, procesamiento, análisis, intercambio y otras transacciones con los datos a fin de establecer responsabilidades.

En ambos casos, Gimbutas y Rodríguez, se ven afectados los principios de consentimiento, licitud, pues la obtención de los mismos no responde a la finalidad inicial de su producción y el deber de confidencialidad y seguridad de los datos.

Recientemente, en el fallo de la Sala II de la Cámara Nacional de Apelaciones Civil y Comercial Federal, en la causa 7870/2007, Luna Silvina Noelia c/Yahoo de Argentina

[14] Artículo 7 – Ley 25.326 de protección de datos personales
[15] C.S.J.N., "Gimbutas, Carolina Valeria c/ Google Inc. s/hábeas data". Fallos 340:1236 (2017)
[16] C.S.J.N., "Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios". Fallos 337:1174 (2014)

SRL y otro s./daños y perjuicios[17], Google y Yahoo fueron considerados responsables de daños a la imagen y al honor de Luna. Este caso, el fallo que data del año 2018, aporta los parámetros con los cuales hoy se asigna responsabilidad a los buscadores de Internet. Este importante Tribunal de Apelaciones resolvió que sólo con la intervención de las empresas demandadas, se logra acceder a información sensible y errónea lesionando el derecho a la intimidad, pues de otra forma, resultaría por completo imposible recabarla ya que sería desconocida por quien realiza la búsqueda.

En este fallo se delimita la responsabilidad de los buscadores de internet definiendo cuál es su incidencia en la divulgación de datos, en este caso no estructurados puesto que son imágenes, sin el consentimiento de la propietaria y en un ámbito que viola su privacidad.

Big data es el resultado de lo que se produce en el ámbito empresarial y administrativo, en las redes sociales y en la internet de las cosas. La Comisión Económica de las Naciones Unidas para Europa, incluye además en este concepto, lo generado por los motores de búsqueda en internet y por dispositivos móviles (Humby, 2006). Así lo entendió también la Justicia argentina en el fallo de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala III de fecha 29 de septiembre 2015, en el caso CEA c/ Google Inc. s/ hábeas data[18], en el que se dispone que el juez debe pronunciarse sobre la obligación del buscador de internet a suministrar los titulares de los blogs injuriantes, con fundamento en la tutela rápida y eficaz.

Aquí se puede observar el tratamiento de las diferentes fuentes de información. El tribunal se debe expedir acerca de si el proveedor de servicios de internet debe aportar los datos de titulares de blogs, siendo que estos no son considerados fuentes de información periodísticas, y solo estas últimas están exceptuadas de brindar dicha información.

En cuanto al derecho al olvido, en el caso Urbandt, Paula c/Banco Río de la Plata S.A. s/amparo, la sentencia 37117/06 del 2008, de la Cámara Nacional de Apelaciones en lo Comercial de la Capital Federal, conformada por Uzal, Miguez y Kolliker Frers, se tratan datos referidos a la historia crediticia. Es decir la finalidad específica de servir para la adopción de decisiones en el mercado del crédito, en el cual una historia negativa cierra las puertas de acceso al sistema (Gils Garbó, 2001).

[17] C.N.A.Civ. y Com. Fed. Sala II "Luna Silvina Noelia c/Yahoo de Argentina S.R.L." (2018).
[18] C.N.A.Civ. y Com. Fed. Sala III "CEA c/ Google Inc. s/ hábeas data" (2015).

El derecho al olvido es definido como el principio, a tenor del cual, cierta información debe ser eliminada de los archivos, transcurrido determinado tiempo desde el momento en que acaeció el hecho a que se refiere, causando su pérdida de virtualidad, omitiendo la evolución, haciéndose intrascendente a los efectos jurídicos relativos a la ejecutabilidad, "para evitar que el individuo quede prisionero de su pasado" (Gozaíni, 2011, P187). En este caso el instituto del hábeas data requerido también se enmarcaría, según la clasificación de Sagués (1995), es el hábeas data aditivo ya que solicita que el banco de datos privado agregue datos donde consten sus cancelaciones, siendo que satisfizo su obligación por lo que su estado de morosidad publicado por el banco de datos perjudica su historial crediticio.

Otro caso que podemos analizar responde a la clasificación de sujetos de la relación de protección de datos personales. Según la Cámara Civil, Comercial, Laboral y Minera de Chubut, en el caso J.F. c/Provincia del Chubut s/hábeas Data s/ Incidente de Apelación, la página web de la Provincia del Chubut no es un registro ni banco dedicada a reproducir datos ya difundidos. Poco interesa en verdad el formato o soporte en que aparezca que la información cuestionada, pues de todas maneras quedaría comprendida en la definición amplia que de archivo, registro, base o banco de datos hace el artículo 2 de la ley nacional 25.326, normativa de orden público esta que en sus capítulos I a IV tiene el carácter de legislación común o de fondo y es aplicable entonces en todo el territorio nacional. Pero lo que no puede faltar para que la que la protección al derecho resulte aplicable es que el dato personal se encuentre incorporado a un registro o banco. Así lo establecen en idénticos términos tanto la Constitución Nacional, artículo 43 párrafo 3, como la Provincial, en su artículo 56 y, coincidente con ellas, el artículo 1 de la ley provincial 4.244 que se refiere a los datos que obren en registros o bancos de datos (Sistema Argentino de Información Jurídica, 2018).

En este caso podemos decir que en el big data se alimenta de este tipo de información, es decir de la ya producida en otros medios y formatos, que posteriormente son reelaboradas y utilizados con un fin determinado, previos procesos de disociación se prioriza volumen más que certeza, se trabaja con márgenes ya que se pretenden establecer tendencias, zonificar, regionalizar, introducir un producto previendo su demanda, estudiar el comportamiento de los consumidores, etc (Peduto, 2014). En caso de que igualmente se pueda identificar al propietario y se recurra a la acción se estarán violando los principios de finalidad, consentimiento, calidad de los datos y confidencialidad, y

dependiendo del tipo de dato se verían comprometidas la seguridad y la intimidad a través de datos sensibles.

Conclusiones Parciales

En este capítulo se analizó la acción de protección de datos personales, desde la ley y desde la jurisprudencia a fin de responder al interrogante ¿Cuáles son los presupuestos con los que los tribunales nacionales, a través de sus fallos, aplican la ley 25.326 en relación al hábeas data y big data?

A tal fin se estableció la procedencia en cuanto a los casos en que se puede recurrir a ella según el artículo 31, del capítulo VII, de la ley 25.326, determinando también quienes son los sujetos legitimados tanto activos como pasivos en esta relación.

También se acudió a la doctrina para establecer en cada caso de incumplimiento, ya sea por omisión, inexactitud, sensibilidad, eliminación u otro, que tipos de hábeas data se pueden aplicar y cuáles son los efectos en los datos y las respuestas de los bancos de datos.

Por otra parte, a través de la jurisprudencia, se detallaron casos de tribunales argentinos, todos posteriores a 1994, año en que se realizó la adición del artículo 43, a la Constitución Nacional incorporando el hábeas data, y otros posteriores a la ley 25.326.

Se pudo observar la evolución de la acción y la gran relevancia que van adquiriendo los temas relacionados a la tecnología y la necesidad de definiciones y conocimientos para diferenciar el origen, la fuente, el medio, los sujetos intervinientes, entre otros. La ley aportó certeza y seguridad a la aplicación del artículo 43, inciso 3, pero debe seguir evolucionando, pues como vimos, el big data tiene dimensión internacional, la tecnología que utiliza es, en muchos casos, externa al país y su soporte se desmaterializa puesto que los datos pueden estar almacenados en cualquier parte del mundo.

Conclusiones Finales

El tema desarrollado en el presente trabajo es sobre el derecho a la intimidad, la protección de datos personales y el big data a la luz del ordenamiento jurídico argentino, en especial a partir de los principios establecidos en la ley 25.326. Por esta razón, el punto de partida fue definir ¿Cuál es el alcance de la ley 25.326 de protección de datos personales en relación al supuesto del uso del denominado big data? Y ¿Bajo qué argumentos normativos el big data entraría en tensión con el derecho a la intimidad y a la protección de los datos personales?

Se puede observar a través del desarrollo de los capítulos que, las actividades de big data, pueden encontrarse reñidas con las disposiciones de orden público de la ley 25.326, con nuestra Constitución Nacional, artículos 19 y 43, inciso 3º, y con tratados internacionales incluidos en el Artículo 75 inciso 22 de la Constitución Argentina.

Una de las tareas de big data es el tratamiento de gigantescos volúmenes de datos de distintos orígenes y fuentes, donde no todos están validados y, regularmente, con falta de consentimiento del usuario. Como vimos, en el artículo 5 de la ley 25.326, para disponer el tratamiento lícito de datos en un banco de datos personales, es menester que el titular del dato haya prestado su consentimiento libre, expreso e informado.

En muchos casos, los proveedores no respetan este principio, por ejemplo, cuando se recolectan y tratan datos sensibles, sin que medien razones de interés general autorizadas por ley, o cuando exista formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles, al no solicitar el consentimiento en caso de cesión o transferencia internacional de datos en favor de terceros que intervienen en aplicaciones o páginas web complementarias a la plataforma de la red social, al presumir el consentimiento del usuario del mero uso que éste hace del servicio, luego de que se hayan efectuado y publicado cambios y cuando se etiquetan contenidos audiovisuales, vinculándolos con el perfil de terceros sin su consentimiento, como en el caso de Luna c/Google.

En los casos precedentes, se observa como el uso de big data vulnera los principios de la ley 25.326, ya que sus fronteras están dispersas en el ámbito internacional. Sobre el ámbito de validez espacial de la ley, el nuevo proyecto[19] se propuso que la legislación establezca su aplicabilidad a todo responsable que realice operaciones de tratamiento de datos de residentes en Argentina, aunque su sede, su base de datos o las operaciones de

[19] Mensaje 147/18 del Poder ejecutivo recuperado de https://www.argentina.gob.ar consultado en septiembre 2018

tratamiento no se encuentren o no se realicen en el país. Esta definición influenciaría ampliamente al ámbito del big data, al igual que los temas relacionados a jurisdicción y competencia. Hoy nuestro ordenamiento jurídico, no alcanza a cubrir eficientemente la protección de los datos de sus nacionales que se encuentran por el mundo, ya que es una tarea titánica revisar los millones de datos que se mueven y manipulan en las redes, cuanto más difícil es para un titular encontrar el origen o el responsable. Por lo que un criterio sería dejar que el actor elija la jurisdicción local o federal para efectuar su reclamo.

Otro punto que el big data debe trabajar, es el de la seguridad, pues en su afán de celeridad y establecer tendencias, puede acarrear daños al propietario, ya que el consentimiento por defecto no existe en estos temas. Con anterioridad a la normativa estudiada, se transfería la responsabilidad de resguardar bajo privacidad sus propios datos personales y eventualmente datos o contenidos de terceros, al usuario, y, por tanto, una renuncia o al menos una limitación a la responsabilidad del productor. Hoy el productor requiere ambos elementos: obtener el consentimiento expreso y brindar seguridad y confidencialidad (Comité de derechos humanos, 2016).

El artículo 9 de la ley 25.326 prevé la obligación del titular de la base de datos de adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

El big data suele utilizar cookies y tecnologías similares para recolectar diversos tipos de datos como dirección IP, fecha de acceso, nombre de usuario, palabras de búsqueda, sistema operativo y tipo de navegador, los cuales permiten ser vinculados a la identidad de una persona, resultando de ello la obtención de datos personales de sus usuarios, los cuales, a su vez, forman parte de bases de datos con fines principalmente publicitarios o que permiten establecer hábitos de consumo. Esto último, a su vez, resulta contrario al principio de calidad de los datos y excede el fin para el cual esos datos fueron recolectados, ya que por lo general al solicitar el consentimiento indican que los fines son de personalización, estadísticos o de seguridad.

El derecho al olvido en el ámbito de big data es un trabajo titánico, puesto que se manejan millones de datos, se relacionan tablas, se intercambia información con otros proveedores, se traspasan barreras internacionales, por lo que estos sistemas deben trabajar desde el diseño para cumplir con la ley.

Por las razones expuestas a lo largo del trabajo, se concluye que los principios de licitud, calidad, consentimiento, información, categorización entendida como manipulación de datos sensibles y de salud, seguridad, confidencialidad, cesión y transferencia internacional se encuentran especialmente comprometidos en los proyectos de big data, principalmente por dos razones: la novedad de estos desarrollos impulsados por los avances tecnológicos y el gran despliegue y manipulación de un volumen extremadamente grande de datos.

Finalmente, llegamos a la conclusión que el big data no protege efectivamente los datos personales y la intimidad cuando ignora o incumple los principios de la ley, exponiendo datos sensibles o no, sin consentimiento y causando un daño a su titular, además vimos que la ley actual no es suficiente puesto que su alcance está restringido y el big data entra en tensión sobre todo en los principios de la transferencia internacional, consentimiento y exactitud.

Al momento de realizar este trabajo se encuentra presentado al Honorable Congreso de la Nación, el anteproyecto de la reforma a la ley 25.346, donde varias de las debilidades de la ley actual se ven superadas, así como también se redefinen términos como datos sensibles o se establecen las acciones a tomar ante determinados eventos llamados incidentes. Por otra parte, mantiene algunos riesgos para el titular de los datos cuando el responsable de la manipulación de los mismos es el Estado.

Pese al panorama bastante desalentador que se ha expuesto a lo largo de este trabajo en cuanto a la protección de datos personales en el ámbito del big data, lo positivo es que, al ser vulnerados estos principios reconocidos en la ley, el titular, o en su defecto el legitimado, puede solicitar la reparación a través de la acción del hábeas data, prescripta en la ley 25.326.

Bibliografía

1. Doctrina

Barrera Buteler, G. (2015). *Derecho Constitucional.* Córdoba: Advocatus.

Bidart Campos, G. (1998). *Manual de la Constitución reformada. Tomo II.* Buenos Aires: Ediar.

Comité de derechos humanos . (2016). El derecho a la privacidad en la argentina. Buenos Aires: Asociación por los derechos civiles.

De Ángelis, C. (2016). *La opinión pública entre la razón y el control social. Una actualización en la era del big data.* (U.d. Aires, Ed.) *Avatares* (11), 9-16. Recuperado el 25 de septiembre de 2018, de http://ppct.caicyt.gov.ar/index.php/avatares/article/view/9199

Doan, A., Halevy, A. & Ives, Z. (2012) *Principles of data integration.* Waltham: Elsevier

Ekmekdjian M., Pizzolo C.(1996), Hábeas Data. El derecho a la intimidad frente a la revolución informática, (Buenos Aires: Ed. Depalma).

Ferreyra E. (2018) *Análisis inicial del proyecto de ley de protección de datos personales de Argentina.* Asociación por los Derechos Civiles. Recuperado el 18 de abril de 2018 de https://adcdigital.org.ar/wp-content/uploads/2018/10/ADC-Analisis-Reforma-LPDP.pdf

Gamero Casado E. (2011) *Las tecnologías de la información y la comunicación en la administración de la justicia.* Pamplona: Aranzadi.

Gandolla , L. (2015). Conflictos entre el big data y la Ley de Protección de Datos Personales. *Sistema Argentino de Información Jurídica*. Recuperado el 14 de septiembre de 2018, de www.infojus.gov.ar

García Barbosa, J., Hernández de Rojas, F., García Esteban, R., Lopez Lopez, V., y Nuñez, M. (2015). big *data. El poder de convertir datos en decisiones.* Madrid: Telefónica.

García Fernández, D. (2015) Metodología de la Investigación Jurídica en el Siglo XXI. En Godínez Méndez, García Peña (Eds.). *Metodologías: Enseñanzas e investigación Jurídicas*. 449.465. Monterrey, México: UNAM.

Gils Garbó, A. (2001). *Régimen legal de las bases de datos y hábeas data.* Buenos Aires: La Ley.

Gozaíni, O. (2006). El proceso de hábeas data en la nueva ley de protección de datos personales. (U. d. Sociales, Ed.) *Revista Jurídica*, 121-152. Recuperado el 08 de

11 de 2018, de http://dspace.uces.edu.ar:8180/xmlui/bitstream/handle/123456789 /412 /El_proceso_de_ hábeas_data_parte01.pdf?sequence=1

Gozaíni, O. (2011). *Hábeas Data. Protección de datos personales. Doctrina y Jurisprudencia. 2ª Edición ampliada y reformada.* Buenos Aires: Rubinzal Culzoni.

Hernández Sampieri, R., Fernández Collado, C. y Baptista Lucio, P. (2010). *Metodología de la investigación* (V ed.). México D.C.: McGraw-Hill.

Herrera, M., Caramelo,G. y Picasso, S. (2015) *Código Civil y comercial Comentado,* Tomo IV. Buenos Aires: Infojus.

Humby, C. (2006). *La vida en datos.* Def Online. Recuperado el 29 de septiembre de 2018, de http://defonline.com.ar/big-data-la-vida-en-datos/

Izcara Palacios, S. (2014). *Manual de Investigación Cualitativa.* México: Fontamara.

Laboratorio de big data. (2014). *Las 5 Vs que caracterizan el big data. Aplicaciones y tendencias que conforman el desarrollo del concepto big data*. Obtenido de https: //bigdata400.wordpress.com/2014/11/11/ las-5-vs-que- caracterizan-el-concepto-de-big-data/

Lezcano, J. (2010) *Las redes sociales en Internet. Herramientas para la comprensión de un fenómeno en progreso,* XI Congreso Nacional y I Latinoamericano de Sociología Jurídica: Multiculturalismo, Identidad y Derecho. Buenos Aires.

Llambías, J. (1997). *Tratado de Derecho civil.* (27 Ed.). Buenos Aires: Editorial Perrot.

Lorenzetti, R. (2015). *Los derechos personalísimos.* (TELAM, Ed). Obtenido de http//www.telam.com.ar/notas/201507/114502-el-nuevo-codigo-civily-comercial -establece-los-derechos-a-la-dignidad-la-intimidad-el-honor-y-la-imagen.html.

Mashey, J. (1998). *The Wave of Infratress Problems.* Solutions Oportunities.

Morello A. (2003) *Avances Procesales.* Buenos Aires: Rubinzal Culzoni.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (s. f.). *Política de Privacidad del sitio*. Recuperada el 16 de septiembre de 2018, de http://www.unesco.org/new/es/culture/themes/illicit-trafficking-of-cultural-property/unesco-database-of-national-cultural-heritage-laws/privacy-policy/.

Oxford University (2013). *The Oxford English Dictionary.* Reino Unido: Oxford University Press.

Palazzi, P. (2008). *El consentimiento para el tratamiento de datos personales en el régimen de la ley 25.326.* Buenos Aires: Astrea.

Palazzi, P. (2004). *La protección de los datos personales en la Argentina. Ley 25.326 de protección de datos personales y hábeas data comentada y con jurisprudencia.* Buenos Aires: Errepar

Peduto, E. (2014). *Big data y la Privacidad. Limitaciones de la ley argentina.* (M. Roca, Entrevistador)

Pérez Sanz, C. (2016). *Aspectos Legales de big data.* Índice. Fundación Dialnet.

Puccinelli, O. R. (2004). *Protección de datos de carácter personal.* Buenos Aires: Astrea.

Puccinelli, O. R. (2014). *El hábeas data de la Constitución Argentina. A veinte años de su inclusión por la Convención Reformadora de 1994*. Pensamiento Constitucional Nº 19, 79-109. Recuperado de http://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/12520.

Puccinelli, O. R. (2017). *El derecho a la Portabilidad de los datos personales. Orígenes, sentido y alcances.* Pensamiento Constitucional Nº 22, 203-228. Recuperado de http://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/19945.

Ques, M. (2014). *Los datos personales y las nuevas tecnologías.* Buenos Aires: Ministerio de educación de la Nación. Obtenido de https://libroelectronicotgd1.files.wordpress.com/2016/12/3-9.pdf

Real Academia Española (2016). *Diccionario de Español Jurídico.* Madrid: Imprenta Real. Recuperado el 18 de marzo de 2018 de https://dej.rae.es/lema/habeas-data.

Red Iberoamericana de Protección de Datos (2017). *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*. Recuperado de https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf.

Sagués, P. (2017). *Manual de Derecho constitucional* (2 Ed.). Buenos Aires: ASTREA.

Sanchez Bravo, Á. (2001). *Internet y la sociedad Europea de la Información. Implicaciones para los ciudadanos.* Salamanca, España: Universidad de Sevilla.

Sistema Argentino de Información Jurídica . (2018). *Dossier. Hábeas data. Selección Jurisprudencia y doctrina.* Ministerio de Justicia y Derechos Humanos. Presidencia de la Nación

Sullivan, C. (2010) *Digital Identity - An Emergent Legal Concept*. Australia: University of Adelaide Press

Valiente, E. (2012). *Génesis histórico-normativa del derecho a la protección de datos personales desde el derecho comparado a propósito de su fundamento.* Tesina de

Máster no publicado. Instituto de derechos humanos: Bartolomé de las Casas. Universidad Carlos III de Madrid.

Witker, J.(1996). *Técnicas de investigación jurídica.* México: McGraw-Hill Interamericana.

Yuni, J. y Urbano, C. (2014). *Técnicas para investigar* (Vol. 1). Córdoba: Brujas

2. Legislación

Nacional

Código Civil y Comercial de la Nación.

Constitución de la Nación Argentina.

Decreto 1558/2001. Reglamenta la Ley de Protección de datos personales. B.O. del 03/11/01.

Ley Nº 25.326. Protección de datos personales. B.O. del 2/11/00.

Ley Nº 21.526 de Entidades financieras. B.O. 14/02/1977.

Ley Nº 20.744 de Contrato de trabajo. B.O.27/09/1974.

Mensaje 147/18. Proyecto de Ley de Protección de Datos Personales. Poder Ejecutivo, Buenos Aires, 19/09/2018.

Internacional

Asamblea General de la Organización de Naciones Unidas (1948) Declaración Universal de los Derechos Humanos (217 [III]) París.

Decisión (UE) 1731/2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales en Argentina.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos (2017). Ley Modelo Interamericana de Protección de Datos Personales. Recuperado el 29/09/18 de http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp.

3. Jurisprudencia

C.S.J.N., “Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios”. Fallos 337:1174 (2014)

C.S.J.N., “Gimbutas, Carolina Valeria c/ Google Inc. s/hábeas data”. Fallos 340:1236 (2017)

C.N.A.Civ. y Com. Fed. Sala III “CEA c/ Google Inc. s/ hábeas data” (2015).

C.N.A.Civ. y Com. Fed. Sala II “Luna Silvina Noelia c/Yahoo de Argentina S.R.L.” (2018).

C.C.A.F. Sala V. “Torres Abad, Carmen c/EN-JGM s/ Hábeas Data” (2018)

C.N.C.C. de la Capital Federal Sala A “Urbandt, Paula c/Banco Río de la Plata S.A. s/amparo” (2008).

C.C.C.L y M. de Chubut “J.F. c/Provincia del Chubut s/hábeas data s/ Incidente de Apelación” (2011).