ISSN 0123-1154

EL FUTURO MARCO LEGAL PARA LA PROTECCIÓN DEL ACCESO A LOS DATOS*

THE FUTURE LEGAL FRAMEWORK FOR THE PROTECTION OF ACCESS TO DATA

VIRGINIA PULDAIN SALVADOR**

Fecha de recepción: 13 de junio de 2017
Fecha de aceptación: 1 de agosto de 2017
Disponible en línea: 30 de noviembre de 2017

Para Citar este artículo/To cite this article

Puldain Salvador, Virginia, *El futuro marco legal para la protección del acceso a los datos*, 47 Rev.Ibero-Latinoam.Seguros, 119-135 (2017). https://doi.org/10.11144/Javeriana.ris47.fmlp

doi:10.11144/Javeriana.ris47.fmlp

* Ponencia presentada como relatoría en el XV Congreso del Comité Iberolatinoamericano de AIDA-CILA, Santa Cruz, Bolivia, mayo 2017.

** Abogada recibida en la Universidad de Buenos Aires (UBA) – Especialista en Derecho de Seguros, Derecho del Consumidor y Riesgos del Trabajo – Autora de Publicaciones y Ponencias en Derecho de Seguros – Miembro titular de AIDA (Rama Argentina) – Vocal de la Asociación para el Estudio del Derecho de Seguros del Interior Argentino (AEDSIA).- Contacto: virginiapuldain@gmail.com

RESUMEN

El presente trabajo busca profundizar en el análisis de "la protección de datos" y los nuevos cambios tecnológicos. Los datos son un recurso fundamental para el crecimiento económico de las naciones y progreso de las sociedades. Las nuevas tecnologías están modificando la forma de informarnos, comunicarnos y relacionarnos. El libre flujo de datos se impone. No obstante, debemos garantizar su protección logrando que la accesibilidad se encuentre debidamente regulada por las autoridades nacionales de cada país. Debemos pensar en la creación de marcos legales que brinden mayor seguridad jurídica en lo que se ha dado en llamar la economía de datos.

Palabras clave: Autodeterminación informativa; Habeas Data; Internet; Privacidad; Protección de datos.

ABSTRACT

The present work seeks to deepen the analysis of "data protection" and new technological changes. Data are a fundamental resource for the economic growth of nations and the progress of societies. New technologies are changing the way we communicate, communicate and relate. The free flow of data is imposed. However, we must ensure their protection by ensuring that accessibility is duly regulated by the national authorities of each country. We must think of the creation of legal frameworks that provide greater legal certainty in what has been called the data economy.

Keywords: Informative self-determination. Habeas Data. Internet. Privacy. Data protection.

SUMARIO

INTRODUCCIÓN

Internet y las nuevas tecnologías están revolucionando el mundo. No sólo la forma en la que nos comunicamos, sino también en la que nos informamos, aprendemos y nos relacionamos. Diariamente aparecen nuevas aplicaciones móviles, redes sociales o dispositivos que facilitan la interacción entre los ciudadanos, empresas y gobiernos.

Se ha ido desarrollando un ideal que hace tan sólo unas décadas hubiésemos pensado que era imposible: la "democratización de la información"**.** En la web no existen límites, niveles socioeconómicos, géneros, razas, horarios ni distancias: todos pueden acceder a ella.

A fines de 2015 la población total de usuarios en **internet** era de tres mil millones de personas y se espera que para el año 2020 esta cifra aumente a los cuatro mil millones, más de la mitad de la población mundial[1].

Marshall McLuhan, considerado como uno de los padres de la teoría de la Comunicación, hablaba hace más de medio siglo de una "aldea global"**[2];** es decir, de un lugar (generado por los medios electrónicos) donde todos los seres están comunicados y perciben como suyos hechos distantes, tanto en espacio como en tiempo.

Hoy la aldea global es una realidad. **Internet**, y en particular las denominadas redes sociales, se han transformado en una inmensa memoria colectiva, ajena a sus protagonistas, que crece sin ningún tipo de control por parte de los dueños de esos datos. La imposibilidad técnica de poder controlar el flujo de información es su realidad actual y nos alerta a ser cada vez más conscientes de los nuevos riesgos que esto implica.

El derecho de las personas sobre la protección de sus datos, íntimamente ligado al ámbito del derecho a la imagen y al honor, se encuentra regulado en la mayor parte de las legislaciones iberoamericanas a través del denominado **habeas data,** en calidad de garantía constitucional. A mayor abundamiento, cada vez son más los Estados que cuentan con

1 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

2 M. McLuhan y B.R. Powers: La Aldea Global, Ed. Gedisa S.A., Barcelona, 1990.

normas específicas en materia de **protección de datos personales**, adaptando el resto de leyes, decretos y otra normativa para una mejor salvaguarda de lo derechos de las personas, así como su tutela judicial efectiva.

En mundo globalizado, en el que la movilidad, no sólo geográfica, si no también económica, profesional, bancaria, juega un papel tan importante, las transferencias internacionales de datos, son una realidad cada vez más frecuente debido a la globalización y geodeslocalización de **Internet** y las nuevas tecnologías como el Cloud Computing.

La protección de la **privacidad** es un derecho fundamental reconocido por las Naciones Unidas que protege la libertad individual, la libertad de expresión, la intimidad y la dignidad personal. Este derecho contiene dentro de sí la **protección de datos** y la figura del **Habeas Data**, según afirma la propia Organización de Estados Americanos.

El Consejo de Europa lo define como un derecho humano fundamental. Por su parte, la Declaración Universal de Derechos Humanos y el Pacto Internacional de las Naciones Unidas sobre los Derechos Civiles y Políticos definen a la **privacidad** como un derecho: «nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación».

La garantía constitucional del **habeas data** impone ciertas obligaciones a las entidades, públicas y privadas, que tratan la información. Los datos recogidos deberán ser utilizados para los fines específicos y explícitos para los que fueron recabados, debiéndose garantizar la seguridad de los mismos y controlando el acceso por parte de personas no autorizadas.

Los ciudadanos tienen derecho a conocer la legalidad en la recopilación de sus datos, quedando estos habilitados para que, en caso de haberse recabado de forma ilegal, puedan solicitar la correspondiente sanción a los responsables. Esta acción constitucional aumenta el nivel de transparencia en el acceso a la información, así como el tratamiento y personas o entidades que acceden o son cesionarios de la misma. Cada vez son más los países iberoamericanos que cuentan con una legislación específica en

materia de **protección de datos**, así como de medios legales y organizativos para proteger el derecho a la **privacidad** y al honor de los ciudadanos.

Iberoamérica avanza en la legislación de un derecho fundamental inherente a las personas, tanto mediante una regulación específica como dentro de la figura de la garantía constitucional del **Habeas Data**, hacia un marco jurídico común que cree un espacio de seguridad jurídica tanto en el ámbito empresarial y las transacciones económicas y de servicios, como de la libre circulación de las personas y sus relaciones más allá de su espacio cotidiano, donde **Internet** y las nuevas tecnologías juegan un papel fundamental y los datos se propagan a gran velocidad y en gran volumen.

1. QUÉ SON LOS DATOS?

¿Qué son los datos? ¿A qué nos referimos con "**protección de datos**"? ¿Sabemos exactamente, qué datos personales nuestros están siendo manejados por las redes sociales o buscadores con los que interactuamos?

Los datos personales son, cada vez más, el activo central para las operaciones de negocios y también resultan esenciales para una administración de gobierno efectiva.

Según normativa de países europeos, se define al dato como toda información sobre una persona física identificada o identificable. Desdenombre y apellido, edad, domicilio, datos financieros, hasta datos sensibles como religión, partido político, orientación sexual o datos sobre la salud.

El "derecho de las personas a la protección de sus datos" se encuentra ligado al derecho a la intimidad, **privacidad**, honor, propia imagen, muchas legislaciones lo reconocen como un "derecho autónomo".

Toda persona tiene derecho a la protección de sus datos de carácter personal. Es decir, tiene derecho a decidir sobre quién tiene datos personales suyos y a saber para qué los usa una organización.

Las herramientas para el procesamiento de datos son cada vez más poderosas y sofisticadas. Asimismo cada vez lo son más económicas, lo

que permite que la información sea fácil de buscar, de vincular y de ubicar para diversos actores, no sólo los gobiernos o las grandes corporaciones.

El bien jurídico subyacente cuando hablamos de "**protección de datos**" es la **autodeterminación informativa**[3], que consiste en el derecho que toda persona tiene a controlar la información que le concierne, sea íntima o no, para preservar de este modo y en último extremo, su identidad, dignidad y libertad.

Basado en la exigencia de "consentimiento" para que la recogida y el tratamiento de datos sean lícitos, el derecho a la **autodeterminación informativa** sobre el que se apoya el concepto de **protección de datos** personales, no sólo entraña un específico instrumento de protección de los derechos del ciudadano, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona y decidir sobre su difusión y utilización por parte de terceros.

2. ACCESO A INTERNET Y ALGUNAS CIFRAS

Un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) del 2016 establece que: en los últimos 5 años, se aceleró el avance de **Internet** en América Latina y el Caribe: 55% de sus habitantes usaron la red en 2015, 20 puntos porcentuales más que en 2010. La penetración de las conexiones en banda ancha también creció fuertemente, particularmente en la modalidad móvil, la que pasó de 7% a 58% de la población. Hay una gran diferencia en los niveles de acceso entre los países de la región.

En promedio, un visitante latinoamericano permanece casi 22 horas en línea mensualmente. En América Latina y el Caribe, el usuario promedio se conecta a **Internet** 21,7 horas por mes, una hora menos que el promedio mundial, de 22,8. Los Estados Unidos y Europa están por encima del promedio mundial, con 35,9 y 25,1 horas en promedio por visitante al mes, respectivamente. En la región, sobresalen el Brasil, con 29,4 horas, y el Uruguay, con 32,6 horas, mientras que en los restantes países se registran entre 15 y 20 horas mensuales por visitante.

3 Chirino Sánchez, Alfredo: Autodeterminación informativa y Estado de Derecho en la Sociedad Tecnológica CONAMAJ, San José, Costa Rica, p. 20, 1997.

México, la Argentina, el Perú, Chile y Colombia están entre los diez países del mundo con mayor porcentaje de usuarios de las redes sociales.

Asimismo, según la Comisión Económica para América Latina y el Caribe (CEPAL): en un segundo, en **Internet** se descargan más de 1.700 aplicaciones, lo que ha llevado a que a finales de 2014, el usuario promedio contara con alrededor de 60 aplicaciones. En el mismo lapso, se realizan más de 44.000 búsquedas en Google y más de 1.700 llamadas por Skype, se envían más de 2 millones de correos electrónicos, más de 300.000 mensajes por protocolo IP a través de WhatsApp y más de 8.500 tuiteos, se efectúan más de 1.800 publicaciones en Tumblr y 50.000 en Facebook, se suben más de 1.900 fotos y se ven más de 98.000 videos en YouTube y 655 horas de video en Netflix.

Total de usuarios de Internet en el mundo: 3.5 mil millones (2015)[4]

País	% Población con acceso
Honduras	18
Guatemala	18
India	19
Cuba	38
Bolivia	39
Perú	41
América Latina y Caribe	54
China	60
Brasil	67
México	80
Chile	84
Uruguay	90
EEUU	91
U.E	93
Argentina	95
Suecia	99

4 https://es.wikipedia.org/wiki/Anexo:Pa%C3%ADses_por_n%C3%BAmero_de_usuarios_de_Internet

No son pocos los que llaman a los datos el "nuevo oro o petróleo del siglo XXI". Existen empresas enteras como los gigantes de **Internet** (Google, Facebook) que basan sus modelos de negocios en los datos[5]. Los datos son su materia prima. Su transferencia es hoy prácticamente instantánea y sin costo, bastando muchas veces un solo click del mouse para mover datos alrededor del mundo.

3. AMÉRICA LATINA Y LA PROTECCIÓN DE DATOS

En los últimos quince años, un número significativo de países de la región han ido incorporando no sólo una legislación específica en materia de **protección de datos** personales sino también, y quizás sea este uno de los aspectos más relevantes, un conjunto de instrumentos organizativos y legales para asegurar unas garantías adecuadas y suficientes y, en consecuencia, una protección efectiva para los ciudadanos.

Argentina, Chile, Colombia, Costa Rica, México, Nicaragua, Perú y Uruguay cuentan con una ley propia en este sentido. Ello ha significado que, en la actualidad, más de ciento cincuenta millones de ciudadanos iberoamericanos disponen, junto al tradicional amparo del **habeas data**, de normas que permiten controlar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías. Sin embargo, y aun reconociendo la gran labor desarrollada en un período tan corto, es evidente que aún queda mucho por hacer y que será necesario diseñar estrategias adaptadas a las necesidades y peculiaridades de aquellos países que aún no cuentan con un marco normativo propio en la materia

Cada uno de los países identificados cuenta con procedimientos particulares para que los titulares de datos personales puedan ejercer los

5 El Congreso de Estados Unidos aprobó el pasado 29 de marzo un proyecto de ley que elimina las garantías de privacidad en la red impuestas por el expresidente Barack Obama y que permitirá a los proveedores de internet vender datos de sus usuarios, como los historiales de búsqueda o la localización. El proyecto, que deberá refrendar en los próximos días el presidente del país, Donald Trump, revoca un reglamento que los demócratas habían redactado para la Comisión Federal de Comunicaciones (FCC, en inglés) y que exigía a los proveedores obtener el permiso de sus usuarios antes de vender sus datos**.** Los republicanos siempre consideraron ese reglamento como un exceso regulatorio y su norma permitirá a los proveedores como Verizon, Comcast y AT&T utilizar por defecto a sus usuarios para competir en pie de igualdad con Google y Facebook en el negocio publicitario en línea, que mueve US$83 mil millones.

derechos que sus constituciones y leyes les reconocen, que van desde el acceso a procedimientos administrativos ante autoridades nacionales de control hasta el reconocimiento de acciones judiciales constitucionales en ejercicio del indicado **habeas data**, reconocido en determinados países como un derecho fundamental directamente aplicable.

El modelo de **protección de datos** personales latinoamericano se encuentra en una fase de transición. La mayor parte de las principales economías de la región cuentan con protecciones constitucionales y leyes comprensivas de protección que regulan el procesamiento de datos personales tanto por el sector público como el privado.

Así y en rasgos generales, la **protección de datos** personales en América Latina aparece como robusta. Sin embargo, los países todavía necesitan trabajar para que sus leyes sean de aplicación efectiva y respondan a los actuales desafíos generados por el desarrollo tecnológico y la cada vez más creciente transferencia internacional de datos personales.

Existen claramente dos bloques de países iberoamericanos, aquellos que no cuentan con legislación sobre **protección de datos** y como mucho en sus textos constitucionales regulan la figura del **Habeas Data**, y aquellos que, o bien tienen Proyectos de Ley en tramitación parlamentaria, o ya cuentan con legislación en materia de **protección de datos** personales

Este segundo bloque de países cuenta con normativas vigentes o en preparación muy influenciadas por la Directiva 95/46/CE y por el Convenio 108 del Consejo de Europa**,** con el fin último de lograr que la Comisión Europea por medio de Decisión reconozca un nivel adecuado de protección.

Recuérdese que Argentina[6] y Uruguay lo tienen reconocido y, asimismo este último ha ratificado el Convenio 108[7], lo que permitiría a priori

6 Argentina fue el primer país de Latinoamérica en haber sido "reconocido" por la Comisión Europea como un país que brinda un nivel adecuado de protección en lo relativo a los datos personales que pueden ser transferidos desde Europa hasta territorio argentino (Decisión 2003/490/EC sobre la adecuación de la protección de los datos personales en Argentina).

7 Convenio Nº 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

afirmar que cuentan con una ventaja competitiva sobre otros países de la región, puesto que al facilitarse las transferencias internacionales de datos (y con ello agilizándose los plazos y reduciéndose los costes y la burocracia), la instalación de una filial de una multinacional en un país u otro de la región, o la contratación un servicio de Cloud Computing dependiendo del lugar de alojamiento del servidor puede decantar la balanza aun lado o al otro.

Ante estos escenarios, la Unión Europea constató que la Directiva 95/46/CE y otra normativa aplicable, no contaban con mecanismos suficientes y adecuados para afrontar los nuevos retos, oportunidades y amenazas en **privacidad** que suponen los avances tecnológicos. Tanto el Big Data, el denominado **Internet** de las Cosas, el Cloud Computing, el aumento de las app, la geodeslocalización, los robos masivos de datos, las brechas de seguridad, los fenómenos virales en redes sociales o aplicaciones de mensajería instantánea o los nuevos tipos delictuales surgen del uso de las nuevas tecnologías como la suplantación o robo de identidad digital, el sexting, la sextortion, el ciberbullying o el grooming. Se impone de este modo replantear escenarios, legislación y modos de protección contra estas nuevas amenazas.

4. NUEVA NORMATIVA EUROPEA. REGLAMENTO UE 2016/679

El pasado 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679[8] del Parlamento Europeo y del Consejo por el que se deroga la Directiva 95/46/CE.

Este reglamento, a diferencia de las directivas, tiene como principal efecto ser de directa aplicación en toda Europa, sin necesidad de incor-

8 El artículo 94 del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) señala que: «1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018. 2.Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento».

poración por los Estados miembros a su ordenamiento interno. Sustituye también a las 28 regulaciones actuales. No obstante, debido a la trascendencia de las nuevas normas y derechos regulados, será aplicable a partir del 25 de mayo de 2018.

Así, durante los dos próximos años, cada Estado europeo y todas las empresas y Administraciones públicas podrán realizar las modificaciones y ajustes necesarios para garantizar su cumplimiento.

La aprobación del RGPD (Reglamento General de **Protección de Datos**) supone la introducción de importantes novedades en materia de **protección de datos** personales, y así, presenta aspectos muy relevantes y positivos. Como es el hecho que supone implantar, por vez primera, una regulación jurídica homogénea y uniforme en materia de **protección de datos** para todos los Estados miembros de la Unión Europea lo que beneficia tanto los consumidores como a las propias empresas, que disponen de una norma única que implantar en todos los países miembros, con la consiguiente seguridad jurídica y transparencia.

Además, el ámbito de protección en materia de **protección de datos**, para los ciudadanos que forman parte de los Estados miembros de la Unión Europea, se amplía de forma considerable desde un punto de vista subjetivo y territorial puesto que ahora con el RGPD se regula no solamente la **protección de los datos** personales de las personas físicas, sino también la circulación de esos datos, y ello no solo en el ámbito territorial de la propia Unión Europea, ya que se extiende también al tratamiento de los datos de los ciudadanos europeos fuera del ámbito de la Unión.

Vale aclarar que en Europa, el derecho a la protección de los datos personales tiene reconocimiento legal como derecho distinto al derecho a la **privacidad**. Varias constituciones nacionales contienen previsiones distintivas en este sentido y, más aún, la Carta de los Derechos Fundamentales de la Unión Europea, adoptada el 7 de diciembre de 2000, establece una clara distinción entre uno y otro derecho. Mientras que el artículo siete consagra el derecho la vida privada y familiar, el artículo ocho reconoce que toda persona tiene derecho a la protección de los datos personales que le conciernan.

La legislación europea consagra la **autodeterminación informativa** como derecho autónomo distinto del de **privacidad**. El nuevo reglamento RGPD tiene dos objetivos principales: a) garantizar transferencias internacionales a países que cuenten con nivel adecuado de protección (deben aprobar un procedimiento particular cada 4 años) b) la libre circulación de datos personales en la Unión Europea.

Principios relativos al tratamiento de datos personales

El RGPD contiene una serie de principios que deberán observarse en todo tratamiento de datos.

- **licitud, lealtad y transparencia:** los datos deberán tratados de manera lícita, leal y transparente en relación con el interesado. Debe entenderse por lícito que el tratamiento se ajuste a lo previsto en la ley y por "transparente" toda la información que se le debe suministrar el titular en ocasión de la recolección de los datos, vinculada a quién es el responsable y su domicilio, qué se harán con los datos y sus posibles destinatarios, carácter facultativo u obligatorio y las consecuencias de proporcionar o no los datos, la posibilidad de ejercer determinados derechos, etc.;

- **limitación de la finalidad:** los datos deberán ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. El tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales;

- **exactitud:** los datos deberán ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;

- **limitación del plazo de conservación:** los datos deberán ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse du-

rante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;

- **integridad y confidencialidad:** los datos deberán ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas;

- **minimización de datos:** los datos deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

En el **RGPD** el consentimiento constituye una de los supuestos por los cuales se considera lícito el tratamiento de datos. Esto significa que si bien es uno de los más importantes, el consentimiento no tiene una preeminencia en el sistema de **protección de datos** de la UE sino que coexiste con otras supuestos legítimos establecidos por la legislación, a saber: si es necesario para la ejecución de un contrato en la que el interesado es parte; si es necesario para el cumplimiento de una obligación legal del responsable del tratamiento; si es necesario para proteger intereses vitales del interesado u otra persona física; si es necesario para el cumplimiento de una misión de interés público o en ejercicio de poderes públicos; y si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, en tanto no prevalezcan los intereses o los derechos del interesado.

El RGPD consagra los derechos tradicionales vinculados a la **protección de datos** personales, como el derecho a la información, el derecho al acceso, el derecho a la rectificación y el derecho a la oposición. Sin embargo, agrega otros nuevos derechos no previstos –o previstos de manera distinta– en los plexos normativos en análisis (excepto en los casos que se indicarán de modo expreso).

- **Derecho a la supresión o "derecho al olvido",** por el cual toda persona tiene la facultad de solicitar la supresión de los datos personales que ya no sean necesarios para el cumplimento de las finalidades

para las que fueron recogidos, cuando se haya retirado el consentimiento y no exista otra base legal para el tratamiento del mismo, cuando el tratamiento haya sido realizado en forma ilícita, etc.

- **Derecho a la portabilidad**, en virtud del cual toda persona tiene derecho a recibir los datos personales que le incumban que haya facilitado a un responsable del tratamiento y a transferirlos a otro responsable, sin que el anterior pueda impedirlo. El interesado puede pedir la entrega de sus datos en un formato de uso común o lectura mecánica o que directamente se le entregue al nuevo responsable, siempre que sea técnicamente posible. México contiene una previsión relativa a la portabilidad de los datos cuando se trata organismos públicos.

CONCLUSIONES Y RECOMENDACIONES

Los datos personales tienen en el contexto actual un rol trascendental, provocado por los profundos cambios acontecidos en el entorno tecnológico y las transformaciones que lo anterior ha ocasionado en las prácticas de las empresas y en sus modelos de negocio, en los cambios organizacionales del Estado y en la modificación de la conducta en línea de los propios individuos.

El aumento sustancial en los flujos transfronterizos motivado en la mayor integración económica y social y el mayor intercambio entre operadores públicos y privados, con más el notorio incremento de la economía digital ha generado un escenario en el que todos estos factores interactúan a tal punto que a veces se torna dificultoso **establecer los límites** entre ellos.

Cada vez más datos de los personas son recolectados, almacenados y son objeto de tratamiento de todo tipo, generando incluso nuevos datos a partir de ese tratamiento de los que el individuo en el que se originó la información ni siquiera está al tanto. No se trata solo de datos o contenido que el sujeto genera de manera consciente, sino también de aquellos datos que genera con cada movimiento que realiza en línea (metadata) y que por lo general desconoce y está más allá de su control.

Y es en este contexto complejo y de cambio vertiginoso en el que confluye el derecho al desarrollo económico y tecnológico de los pueblos,

la libre iniciativa, y la libertad de competencia, pero también el derecho a la libertad de expresión, de comunicación y de opinión; el derecho a la inviolabilidad de la intimidad, de la vida privada, del honor y de la imagen; el derecho de acceso a la información; el derecho la **privacidad** y de la **autodeterminación informativa.**

El consentimiento tiene un papel fundamental en todo este entramado y su regulación entendemos es la clave de bóveda para la protección de los datos personales. Concientizarnos, tener más información para adoptar medidas de prevención. Solicitar el consentimiento para cada finalidad. En un proceso de compra venta on line, una cosa es el consentimiento para la compara en sí, otra el consentimiento para el envío de publicidad y otra la cesión de datos a terceros. Más aún si esos datos son sensibles.

Revisar los formularios, adaptarlos, hacerlos más amigables. Habilitar por ejemplo distintos botones para marcar en función de la finalidad que se trate la aceptación o no. Actualmente se incluye todo junto y en la mayoría de las ocasiones, el titular del dato no es consciente que firma un cheque en blanco con sus datos.

Por último, cabe destacar que las herramientas de enforcement, es decir, aquellas que permiten la aplicación efectiva de las garantías, derechos y protecciones que consagran la normativa, son en general deficitarias.

La necesidad de fortalecer los estándares de protección de los datos personales y sus mecanismos de enforcement lo consideramos prioritario. Dado el contexto descripto, la ponderación y adopción de nuevas previsiones aparecen como necesarias en pos del fortalecimiento de los estándares hoy por hoy vigentes. Figuras como la de los principios de minimización y responsabilidad proactiva o el derecho a la portabilidad, como así también el mayor detalle y análisis de viabilidad de medidas concretas en cabeza de los responsables que aseguren el mejor tratamiento posible de los datos personales se presentan como de discusión necesaria. La generación de vías más efectivas de información para el individuo, que sea clara, concisa y pertinente y le posibilite la comprensión acabada de la suerte de sus datos personales es todavía materia pendiente. Proponemos entonces, regular donde no se ha hecho y modificar donde sí se hizo.

BIBLIOGRAFÍA

M. McLuhan y B.R. Powers: La Aldea Global, Ed. Gedisa S.A., Barcelona, 1990.

Chirino Sánchez, Alfredo: Autodeterminación informativa y Estado de Derecho en la Sociedad Tecnológica CONAMAJ, San José, Costa Rica, p. 20, 1997.

Ekmekdjian, Miguel Ángel, Tratado de Derecho Constitucional, p. 567, tº I, Editorial Depalma, Buenos Aires, 1993.

Bidart Campos, Germán, "¿Habeas data, o qué? ¿Derecho a la verdad, o qué?" La Ley - A, pág. 212.1999.

Informe: Estado de la Banda Ancha en América Latina y el Caribe 2016 – Cepal – Naciones Unidas. Recuperado 09/2016.0https://drive.google.com/file/d/0BxCBD5ri9y9UekhhWGlFZFJOMkE/view