**Título** Datos Personales, marketing digital y los derechos de los ciudadanos en América Latina

**Tipo de Producto** Ponencia (texto completo)

**Autores** Villan, Marco Antonio & Bosque, Lía

Ponencia presentada en el VI Congreso Internacional de Ciencias Sociales - Cancún, México

## Código del Proyecto y Título del Proyecto

C19S23 - Marketing Digital y protección de datos personales en la era del Big Data en Latinoamérica

## Responsable del Proyecto

Villan, Marco Antonio

## Línea

Tecnologías de la Comunicación y la Información

## Área Temática

Derecho

## Fecha

Noviembre 2018

**INSOD**
Instituto de Ciencias Sociales y Disciplinas Proyectuales

FUNDACIÓN UADE

# DATOS PERSONALES, MARKETING DIGITAL Y LOS DERECHOS DE LOS CIUDADANOS DE AMÉRICA LATINA

## Estado de protección de los datos de los ciudadanos

Personal data, digital marketing and the rights of citizens of latin america

Lia Bosque [1]
[1] Universidad Argentina de la Empresa (UADE). Instituto de Ciencias Sociales y Disciplinas Proyectuales (INSOD). Buenos Aires, Argentina.

Marco Antonio Villan [1]
[1] Universidad Argentina de la Empresa (UADE). Instituto de Ciencias Sociales y Disciplinas Proyectuales (INSOD). Buenos Aires, Argentina.

KEY WORDS

*Data Protection*
*Privacy*
*Personal Data*
*GDPR*
*Digital Marketing*
*Latin America*

ABSTRACT

*The impact of the entry into force of the General Data Protection Regulation introduced a new panorama in Latin America. Countries seek to adapt to regulations and citizens must adapt to new conditions of use of services abroad.*

*The article will analyze the countries that are in the process of updating and adapting to the RGPD. In addition, we will work on the protection of data and the processing of data for marketing, such as its regulation and updating based on European regulations.*

PALABRAS CLAVE

*Datos Personales*
*Privacidad*
*Protección de datos*
*RGPD*
*Marketing digital*
*América latina*

RESUMEN

*El impacto de la entrada en vigor del Reglamento General de Protección de Datos Personales de la Unión Europeo introdujo un nuevo panorama en América Latina. Los países buscan adecuarse a la normativa y los ciudadanos deben adaptarse a nuevas condiciones de uso de servicios en el extranjero.*

*En el artículo se analizarán los países que se encuentran en fase de actualización y adecuación a la RGPD. Además, se trabajará sobre la protección de los datos y el tratamiento de datos para marketing, como su regulación y actualización en base a la normativa europea.*

Aceptado:11/09/2019

# 1. Introducción

Las tecnologías de la Información y la Comunicación produjeron en las últimas décadas una serie de cambios de paradigmas en la forma de hacer marketing, su relación con los consumidores, la recopilación de la información y los grandes almacenes de datos que constituyen el Big Data. Con la aparición del motor de búsqueda de Google surgió la posibilidad para el usuario promedio de buscar una amplia cantidad de información sobre una empresa o producto desde la comodidad del hogar, a su vez la recopilación de perfiles de navegación es cada vez mayor en los últimos 30 años, por lo que, si bien se aceptan condiciones de uso de diferentes servicios, en sectores vulnerables como en los niños, niñas y adolescentes el impacto a la privacidad de aún mayor.

Entre los cambios que también surgieron en las últimas dos décadas es la recopilación y análisis en forma masiva de información o Big Data, la minería de datos para analizar consumidores y la inteligencia artificial. Los procesos de análisis masivos es un debate ético sobre su uso, pero existe el problema de los datos públicos, aquellos datos que son subidos por los jóvenes que van desde las redes sociales, foros, comentarios y todos datos con los que se puedan identificar a la persona. Las últimas décadas también trajeron consigo el debate de la privacidad en el ámbito digital y una necesidad por implementar un marco normativo que proteja los derechos de los ciudadanos.

La recopilación de datos ocurre desde múltiples fuentes que van desde los dispositivos móviles, la geolocalización, redes sociales, datos públicos y privados, recopilación por radiofrecuencia, domótica y sistemas de la información que involucran datos de individuos.

Así como el derecho humano de acceso a Internet es un derecho fundamental y derecho humano, también existe el derecho a la intimidad y habeas data como derechos personalísimos que poseen todos los individuos al nacer ya que tienen la característica de ser innatos. De esta forma, a pesar de los avances tecnológicos se deben garantizar estos derechos.

Las primeras normativas de protección de datos surgieron en la década del sesenta y setenta. Según un análisis de la Organización para la Cooperación y Desarrollo Económico (OCDE) el volumen y múltiples usos de los datos en los últimos 30 años han sido abrumadores debido a que las tecnologías de la información han mejorado la capacidad de procesamiento, almacenamiento, análisis y transferencia de datos.

Otros de los aspectos críticos en materia de regulación es la recopilación de datos de niños, niñas y adolescentes. Desde 1998 existe la Ley sobre Protección de la Privacidad de los Niños Online, también llamada COPPA. Esta ley se desarrolló en una etapa donde aún no existían las redes sociales, los dispositivos móviles y en donde aún no se pensaba en las cantidades masivas de datos. Por otro lado, para ese año en américa latina aún no existía ninguna regulación,

La innovación de COPPA fue que no permitía la recopilación de datos, incluidos audios, videos y fotos y todo tipo de información de personas menores de 13 años.

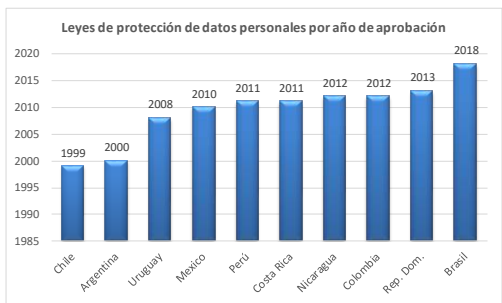
A diferencia de la Unión Europea América Latina presenta un doble desafío: por un lado, la necesidad de actualización de normativas que tienen casi dos décadas de vigencia o más y países que aun no poseen una legislación específica. El impulso del Reglamento de Protección de Datos Europeo impulsó cambios para estandarizar el cuidado y la protección de datos personales. Por otro lado, todas las empresas de américa latina que almacenan y procesan información personal sobre ciudadanos de la UE deben actualizarse para proteger los datos personales independientemente en donde estén y hasta incluso si son datos en la nube.

# 2. Marco legal de protección de datos en América Latina

La región no tiene una ley homogénea como es el caso de la Unión Europea que posee el Reglamento General de Protección de Datos Personales que entró en vigor el 25 de mayo de 2018.

Como se puede apreciar en la figura 1 Chile en 1999 fue uno de los primeros países de Latinoamérica con una ley de protección de datos. Posteriormente en el año 2000 Argentina aprueba la Ley 25.326 con la que posiciona al país con una legislación que incluye un Registro Nacional de Bases De Datos, un órgano de control y una adecuación aprobada el 30 de junio de 2003 con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

Figura 1. Estado actual de leyes de protección de datos personales en América Latina



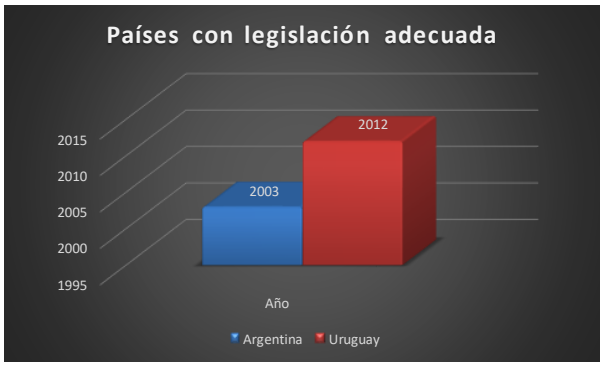

Fuente(s): Bosque Lía, Villan Marco Antonio, 2018.

Esto significa que, al haber transferencias internacionales de datos, la legislación, en este caso el Reglamento General de Protección de Datos de la Unión Europea se transporta con esos datos y se seguirán aplicando con las garantías que los estados de la Unión Europea ofrecen.

El análisis también supone que los países de Latinoamérica se encuentran con leyes que se podrían considerar desactualizadas, teniendo en cuenta el desarrollar de nuevas técnicas y formas de recopilación de información, además de que también existen nuevas amenazas que atentan contra la integridad, confidencialidad y disponibilidad de los datos.

Como se puede ver en la figura 2 sólo dos países poseen legislación adecuada en América Latina, además de Argentina en 2012 se incorporó Uruguay como un país con adecuación. De esta manera, mediante una decisión de adecuación se declara que un estado ofrece un nivel de protección adecuado y por tal razón se pueden transferir datos a otra empresa en un estado que no pertenezca a la Unión Europea.

Figura 2. Países con legislación adecuada en América Latina




Fuente(s): Bosque Lía, Villan Marco Antonio, 2018.

Si se quisiese realizar una transferencia internacional desde la unión europea a estos dos países no habría que establecer garantías adicionales, caso contrario si hay que realizarlas.

### *2.1. Brasil y Chile: el impulso de los nuevos estándares en la región*

El 29 de mayo de 2018, cuatro días después de la entrada en vigencia del RGPD de la UE, se aprobó el proyecto de Ley N° 4060/2012 que establece una ley general de protección de datos personales en Brasil. La aprobación de la ley supuso un adelanto para la región y la implementación de una ley con características similares a la ley europea.

La ley de Brasil propone que la legislación sea aplicable a empresas que tienen sede en dicho país y realicen recolección de datos en el territorio brasileño. Además de requerir el consentimiento del ciudadano para el tratamiento de los datos, también se deben brindar las herramientas para que el usuario de los datos pueda acceder, corregir o eliminar toda la información.

También, incorpora buenas prácticas para que empresas con sede en Brasil incorporen procedimientos de adecuación y compliance. En caso de incumplimiento de la norma se estima que las sanciones incluyen multas altas como el 4% de los ingresos de la compañía en Brasil, limitados a 50 millones de reales. También se le prohibirá la recolección de datos y actividades de tratamiento direccionadas en Brasil.

Por otra parte, Chile incorporó en 2018 nuevos principios al proyecto de ley aprobado que modifica la Ley 19.628. Entre las novedades surge la modificación al alcance de dato personales, ahora se refiere a cualquier información vinculada o referida a una persona natural, identificada o identificable. De esta manera, la identificación también incluye a datos combinados. También, modifica el consentimiento y lo define como voluntad libre, específica, inequívoca e informada. Eliminan el consentimiento escrito.

También, establece una distinción entre cesión de la comunicación de datos personales. Menciona que la cesión es el traspaso entre responsables de bases de datos. Por otro lado, la comunicación involucra el dar a conocer los datos sin llegar a cederlos entre responsables.

Entre los artículos más destacados se encuentran también aquellas categorías especiales para el tratamiento de los datos personales como pueden ser los datos de niños, niñas y adolescentes; los que se utilizan con fines históricos, estadísticos o científicos; y datos de geolocalización. También regula los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Entre los deberes que se agregaron en la nueva ley para los responsables del tratamiento de datos se encuentran la seguridad de los datos, deben aceptar medidas técnicas y organizativas para evitar violaciones a las medidas de seguridad y la obligación de reportarlos.

Para todos estos casos también hay aumentado las sanciones contra aquellos responsables de bases de datos no cumplan la normativa.

### *2.2. Datos sensibles en Brasil*

Los datos sensibles son los relacionados a datos personales 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.

En la Ley de Brasil se incorporó, al igual que el Reglamento de Protección de Datos Personales de la Unión Europea, a los datos genéticos o biométricos como datos sensibles.

### *2.3. México y la Ley de protección de datos personales en posesión de sujetos obligados*

México también endureció su normativa y en abril de 2018 se aprobó la Ley de Protección de Datos Personales en posesión de sujetos obligados.

La ley tiene como objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, que son considerados por ley en el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. El estado garantizará la protección de los datos personales de sus titulares.

Al igual que las leyes de Brasil y Chile y con diferencia de otras regulaciones de la región, se incluye a la información genética como un dato sensible.

Esta ley se podría enmarcar en la política que hay en la región de transparencia, de acceso a la información pública, de gobierno y de datos abiertos.

### *2.4. La importancia de los derechos ARCO y los ciudadanos*

Los derechos ARCO consisten en Acceso, Rectificación, Cancelación y posición. Para comprenderlos primero hay que reflexionar sobre la titularidad de los datos. Todos los ciudadanos que brinden sus datos personales a terceros no dejan de ser titulares de los mismos, poseen derechos y garantías por sobre los que realizan el tratamiento de los datos, ante el sujeto obligado que esté en posesión de los mismos. Argentina, Brasil, Chile, Colombia y México son los países que tienen estos derechos incorporados en su normativa.

El derecho de acceso es la facultad que tienen los ciudadanos de poder exigir información sobre sus datos personales a los responsables de una base de datos si están siendo tratados. En tal caso, se deberá determinar cuáles son los fines del tratamiento, el origen en que se recopilaron los datos y las comunicaciones realizadas o previstas.

Un segundo derecho es el de rectificación. Esto significa que todo ciudadano puede exigir al responsable de una base de datos que su información personal pueda ser modificada, actualizada o rectificada en caso de que sean inexactos, erróneos, s o incompletos. En estos casos se deben presentar la información referida para su corrección de la rectificación solicitada.

El tercer derecho que posee un ciudadano es la de cancelación. En el caso que el titular de los datos personales considera que sus datos contravienen el marco normativo o de que sus datos han dejado de ser necesarios para la finalidad de la base de datos, puede solicitar la cancelación o eliminación de sus datos en un plazo estipulado.

Por último, el titular de los datos posee el derecho de oposición. Puede oponerse al tratamiento de los datos si se hubiesen recabado sin su consentimiento o cuando existen motivos fundados para ello.

### *2.5. Ampliación de los derechos ARCO con el Reglamento de Protección de Datos Personales de la UE*

EL RGPD incorporó a la normativa dos nuevos derechos como son el de portabilidad de los datos y el olvido.

El derecho a la portabilidad de los datos hace mención a que el usuario puede solicitar la información y la debe recibir en un formato estructurado, de uso común, de lectura mecánica e interoperables. Se debe alentar a los responsables a crear formatos interoperables que permitan la portabilidad.

En cuanto al derecho al olvido se realice un refuerzo en los entornos en línea. En su artículo 66 dice que el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales está obligado a indicar a los responsables del tratamiento que estén tratando tales datos que supriman todo enlace a ellos o a las copias o réplicas de datos. De esta forma, se contempla el derecho al olvido cuando existen datos que pueden comprometer el derecho al honor y a la intimidad de los ciudadanos.

### *2.6. Anteproyecto de ley de protección de datos personales en Argentina*

En la actualidad existen dos países que se encuentran trabajando con anteproyectos para la actualización de su normativa. Uno es Honduras que se en un proceso más avanzado de aprobación ya que el Congreso Nacional aprobó una serie de artículos entre abril y noviembre de 2018.

Por otra parte, en Argentina que se encuentra en debate desde el año 2016 el anteproyecto de protección de datos personales, que al igual que el resto de los países de Latinoamérica se alineará a la normativa de la Unión Europea (Agencia de Acceso a la Información Pública, 2017).

### *2.5. Honduras y sus cambios en la legislación*

Durante 2018 el Congreso Nacional se encuentra en debate y lleva unos 36 artículos de los 97 que posee el proyecto de Ley de Protección de Datos Personales. Este debate plantea con su aprobación que los ciudadanos sean los responsables y tengan los derechos a decidir, cómo y quien va a tratar su información personal (El reportero, 2018).

## 3. RGPD y las nuevas obligaciones para las empresas, administradores y otras entidades

La nueva regulación impuso nuevas obligaciones para los responsables de la administración y tratamiento de las bases de datos.

Se pueden destacar en carácter de obligatoriedad la incorporación de la figura de un Delegado de Protección de Datos (DPO) interno o externo que asista a las organizaciones para que cumplan la norma.

En cuanto a la seguridad de los datos y a la privacidad se deberán realizar evaluaciones de impacto sobre la privacidad para determinar los riesgos que supone tratar datos y también establecer medidas para mitigar o eliminar riesgos. Además, se deberán informar las brechas de seguridad a las autoridades de control y en casos graves a los afectados tan pronto sean conocidas en un plazo de 72 horas.

También incorporaron cambios respecto a los datos sensibles, estos se amplían y se protegen ahora los datos genéticos y los biométricos. Este punto también fue incorporado en la Ley de Protección de Datos de Brasil.

Por otro lado, desaparece la obligación e inscribir los ficheros y se sustituye por un control interno y un inventario de las operaciones de tratamiento de datos que se realicen.

En relación con las transferencias internacionales se establecen garantías más estrictas y mecanismos de seguimiento en relación con las transferencias internacionales de datos fueras de la Unión Europea.

Por último, las sanciones se endurecieron y el incumplimiento de la ley supone llegar a los 20 millones de euros o el 4% de la facturación global anual.

## 4. Privacidad desde el diseño y por defecto

Ann Cavoukian desarrolló el concepto de Privacy By Design (Cavoukian, 2011) o privacidad desde el diseño, el cuál finalmente fue incorporado en el Reglamento General de Protección de Datos, como un tema pendiente ya que con la nueva normativa se agravan las penas para aquellos que no lo cumplan.

La privacidad desde diseño significa que la protección de los datos del usuario debe ser considerada desde la fase inicial de un proyecto tecnológico, por ejemplo, si se va a pensar en desarrollar una aplicación que recopile información personal, se debe planificar cuáles van a ser las medidas de privacidad desde el diseño, así como también la seguridad de las mismas.

Por otro lado, la privacidad por defecto significa que los datos que sean recolectados serán para determinado proyecto y serán resguardados con las máximas medidas de privacidad por defecto.

Estas garantías deben ser aplicadas durante las fases de desarrollo y producción, así como también en el ciclo de vida de los datos personales (desde su recolección hasta su destrucción). También, hay que tener en cuenta a los usuarios y tener un especial cuidado con los datos que recopilan de personas menores, por lo que tanto el tratamiento como el resguardo debe ser especial contemplando la normativa de cada país donde se tienen los servidores o desde donde se brindan los servicios.

### *4.1. Privacidad por defecto y diseño en el Reglamento General de Protección de Datos Personales de la Unión Europea*

La importancia que radica en la normativa europea es la incorporación de la privacidad desde el diseño y por defecto en el artículo 78. De esta manera, se debe garantizar la reducción del tratamiento de los datos personales, seudonimizar los datos personales y dar transparencia a las funciones y el tratamiento de datos personales, así como también mejorar los elementos de seguridad. (Diario Oficial de la Unión Europea, 2018)

Por otro lado, al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que realizan tratamiento de datos personales o están basados en el tratamiento se debe alentar a los desarrolladores y productores de servicios y aplicaciones que diseñen y aseguren la debida protección de los datos. Deben tenerse en cuenta los principios desde el diseño y por defecto. Esto se debe realizar desde el inicio y planificación de un proyecto como regla.

### *4.2. RGPD y los principios de transparencia y responsabilidad*

Con la introducción de estos nuevos principios las empresas y todos aquellos que recopilen datos personales deben implementar mecanismos que permitan acreditar que se adoptan las medidas necesarias para tratar los datos personales. Además, se sostiene que debe existir una responsabilidad proactiva.

## 5. Sectores vulnerables: privacidad y consentimiento de niños, niñas y adolescentes

Según un estudio realizado en 2018 por la Organización de Consumidores y Usuarios (OCU),

organización española sin fines de lucro, el 88% de los usuarios brinda el consentimiento en las condiciones de uso en Internet sin leerlas. El principal motivo es el lenguaje complejo en que están escritas para aceptar sin leer. Por otro lado, el 91% de los encuestados denunció que a la hora de registrarse a un servicio en línea a veces se les piden datos que no tienen que ver con dicho servicio, estos datos suelen ser utilizados con un provecho comercial de los clientes y ganancias. En ocasiones suelen ser utilizados también para realizar marketing dirigido a perfiles de todas las edades.

### *5.1. América del sur y la protección de los niños, niñas y adolescentes*

Para ejemplificar se analizarán 3 casos: se analizarán las normativas más actualizadas como es el caso de Chile y Brasil, y por el otro se mencionará la ley argentina que tiene en tratamiento su anteproyecto de Protección de Datos Personales.

En el caso de Chile, con la reforma de la Ley 19.628, los datos personales de niños y niñas establecen a personas menores a 14 años y para su recopilación se solicita una autorización de padres y adolescentes. En el caso de los adolescentes, personas menores entre 14 y 18 años, tendrán el mismo tratamiento que los adultos a excepción de sus datos sensibles que deberán ser objeto de autorización de sus padres o sus representantes.

En el caso de Brasil y la ley 13.709, posee un apartado especial sobre niños y adolescentes en la sección III, artículo 14. Sostiene que el tratamiento de datos personales debe realizarse con el consentimiento específico y destacado dado por al menos uno de los padres o responsables legal. Además, todos aquellos que realizan tratamiento de datos de personas menores deberán mantener pública la información sobre los tipos de datos recolectados y la forma de utilización y los procedimientos para el ejercicio de los derechos de acceso. Otro artículo importante es que las empresas o los responsables de recopilar los datos no deberán condicionar la participación de los titulares en juegos, aplicaciones de Internet u otras actividades al suministro de informaciones personales más allá de las necesarias para la actividad.

La regulación brasileña incorpora también que las empresas deben hacer esfuerzos razonables y tecnológicos para verificar la edad de los niños, niñas y adolescentes. Además, deben brindar informaciones claras y accesibles, con el uso de recursos audiovisuales cuando sean necesarios para proporcionar la información necesaria a los padres o al responsable legal para entendimiento de las personas menores.

En tanto, el Reglamento de Protección de Datos de la Unión Europea menciona en su Artículo 38 que los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente al niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente al niño.

También, se establecen pautas para el tratamiento de los datos personales para aumentar la privacidad de los usuarios menores. Si bien se puede fijar la edad por país, será legal siempre y cuando estos tengan más de 16 años, el reglamento permite bajar la edad y que cada miembro de la Unión Europea establezca siempre con un límite inferior de 13 años, en el caso de menores de esas edad se necesitará el consentimiento del titular de la patria potestad, lo que aún no queda claro es cómo se va a determinar la identidad para verificar el cumplimiento de ese requisito del consentimiento y en realidad no es un menor modificando los datos.

Por último, también si se van a recopilar datos de menores de edad además de que el consentimiento debe ser verificable, el aviso de privacidad tiene que estar escrito en lenguaje claro para que los niños, niñas y adolescentes puedan comprender que van a hacer con sus datos en el caso de que quieran ejercer sus derechos de acceso o rectificación, bloqueo o supresión.

### *5.2. Interpretación de las normas en lenguaje claro*

El lenguaje Claro es clave para que el significado de los derechos y obligaciones de los ciudadanos sea comprensible. Estás deben realizarse con información concisa, accesible y fácil de entender. Deberían ser realizadas en un lenguaje claro no sólo para los adultos sino también de manera específica para los niños, niñas y adolescentes.

Según la International Plain Language Federation el lenguaje claro o llano es:

> Una comunicación está en lenguaje claro si la lengua, la estructura y el diseño son tan claros que el público al que está destinada puede encontrar fácilmente lo que necesita, comprende lo que encuentra y usa esa información

La comunicación en términos fáciles que permitan al lector comprender los términos jurídicos facilitarían la lectura de condiciones de uso y los contratos digitales que aceptan los usuarios sin leer.

También como se mencionó anteriormente en le regulación europea hay una exigencia por la posibilidad de solicitar a los responsables del

tratamiento de las bases de datos, toda la información relativa al titular y en bases de datos estructuradas y en forma clara. Ya no solo se exigen las normas en lenguaje claro sino también cuando el usuario accede a la información, la misma está disponible y en un lenguaje entendible.

### *5.3. Argentina y el anteproyecto de protección de datos personales para el tratamiento de datos de niños, niñas y adolescentes*

En Argentina, la ley 25.326 de protección de datos personales no tiene ese grado específico sobre el tratamiento de los datos de los niños. Si, en el anteproyecto de Ley de protección de datos personales presentado por la Agencia de Acceso a la Información Pública, en el artículo 18 se trata sobre el tratamiento de datos de niños, niñas y adolescentes (Agencia de Acceso a la Información Pública, 2017). Según el artículo, en el tratamiento de datos personales de un niño, niña o adolescente, se debe privilegiar la aplicación del superior interés del niño, conforme a la Convención sobre Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

Sostiene también, que es válido el consentimiento de un niño, niña o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios digitales al alcance de sus gustos y necesidades. Al igual que la Ley Coppa, el consentimiento es lícito si el niño, niña o adolescente tiene como mínimo trece años. Si el niño es menor de trece años, tal tratamiento únicamente se considera lícito si el consentimiento fue otorgado por el titular de la responsabilidad parental o tutela sobre el niño, y sólo en la medida en que se dio o autorizó. En este punto, existe siempre el riesgo de que el menor a la hora de aceptar condiciones de uso complete los datos utilizando otra edad para poder acceder al servicio sin el consentimiento de los adultos. El problema de garantizar la edad del usuario sigue siendo un factor de polémica, aunque la ley sostenga que el responsable del tratamiento debe realizar esfuerzos razonables para verificar que el consentimiento haya sido otorgado por el titular de la

## 6. Marketing digital, RGPD y América Latina

En este último punto se analizan como impacta la nueva norma en América Latina teniendo en cuenta que si hay filiales extranjeras que realizan publicidad y marketing directo deben adaptarse para cumplir con los nuevos lineamientos. Los ciudadanos suelen ser acechados por publicidad contextual cuando navega en Internet, revisa correos electrónicos y utiliza los dispositivos móviles, debido a la gran cantidad de formatos de anuncios que existen hay un seguimiento de las empresas a los consumidores, esto trae consigo aparejado el problema a la privacidad. Según un estudio realizado por HubSpot sólo el 36% de los profesionales del marketing son conscientes del RGPD, mientras que el 15% de las empresas no han tomado medidas al respecto y corren riesgo de incumplimiento. (Hubspot, 2018)

### *6.1. Recopilación y almacenamiento de los datos*

El RGPD sostiene el principio de transparencia, donde se exige que toda información dirigida al público sea fácil y accesible de entender, que se utilice un lenguaje claro y sencillo. Es importante que la información sea trasmitida mediante un sitio Web o por otro medio porque es muy difícil saber quién recoge los datos, por quién y cuál es la finalidad, que datos personales le conciernen y como es en el caso de la publicidad en línea (Martinez Molera, 2018).

También, las empresas que recopilan datos deben introducir la reducción de datos, si bien siempre que se ingresa a una Web hay posibilidades de obtener una conversión una posible venta. Hay que tener en claro que sólo se puede recabar información que sea adecuada, relevante y limitada para el propósito de la recolección, si se considera excesivo será considerada una infracción.

Una vez obtenida la información las empresas y los responsables de bases de datos pueden usar la información que recopilan, con previo consentimiento por parte del usuario, sólo para los propósitos específicos, explícitos y legítimos. No pueden utilizarla con otro propósito para el que se recopiló, transferirla o compartirla. En el caso que deseo realizarlo debe realizarle con el consentimiento del interesado.

### *6.1. Fin del ciclo de vida de los datos personales*

Una vez finalizada la relación contractual con los responsables de recopilar los datos personales se deben tener en cuenta la eliminación de los datos de los servidores donde son tratados, de sistemas informáticos propios y de servidores de terceros. No debe tener una retención salvo que tenga un plazo estipulado por el cual se recopilaron. En

### *6.2. Seguridad de los datos*

La seguridad informática y la seguridad de la información es un aspecto fundamental para proteger la información en medios informatizados. De esta manera, las empresas deben adoptar medidas técnicas y organizativas para proteger los datos personales del procesamiento no autorizado,

su divulgación, acceso, destrucción, alteración o pérdida accidental. Se podrían utilizar técnicas como el cifrado o métodos de seudonomización y anonimización para protegerlos o separar los datos de otro tipo de información del sistema.

### *6.3. Argentina y la actualización de las medidas de seguridad para el tratamiento y conservación de los datos personales en medios informatizados*

Mediante la Resolución 47/2018 se aprobó en Argentina una serie de medidas de seguridad que deben seguir las empresas para mejorar las prácticas de recopilación de datos, los controles de acceso, la gestión de recuperación de información, los controles de cambios, la gestión de vulnerabilidades, la destrucción de la información y el manejo de incidentes de seguridad.

## 6. Conclusión

Existe una necesidad de actualización en Latinoamérica acorde a los estándares internacionales de protección de datos personales. Es necesarios, un trabajo unificado con la experiencia de la Red Iberoamericana de Protección de Datos Personales para establecer pautas y lineamientos de trabajo que mejoren el tratamiento y cuidado de los datos en la región.

Se pudo identificar durante el presente documento que una gran parte de países latinoamericanos no se encuentran actualizados en materia de protección de datos de los usuarios y existen normativas, como el caso de Argentina, que tienen aproximadamente 18 años sin actualizar su normativa vigente. Pese a tener actualizaciones en materia de seguridad y de la creación de una Agencia de Acceso a la Información Pública, su anteproyecto aún se encuentra en debate para su aprobación.

En materia de adecuación de normativas, existen sólo dos países que son considerados países adecuados para la Unión Europea (UE) uno es Uruguay y otro es Argentina. De esta forma para la transferencia internacional de datos entre estos países y países de la UE no serían necesarios contratos internacionales.

Por otra parte, existe un problema fundamental que también se pudo analizar y es que las empresas y la industria deberían desarrollar políticas de privacidad y términos y condiciones de forma más atractiva para que los ciudadanos de todas las edades puedan informarse correctamente sobre cuál va a ser el destino de la información al aceptar las condiciones de uso y privacidad de una aplicación o servicio. Se debe brindar transparencia en la recopilación de datos que las empresas realizan. Especialmente en el tratamiento de datos de niños, niñas y adolescentes ya que las normativas actuales y las que están en proceso de desarrollo protegen especialmente a los sectores vulnerables.

La privacidad desde el diseño y por defecto tuvo mayor impacto y dejo de ser una práctica optativa ya que con el Reglamento General de Protección de Datos Personales (RGPD) paso a ser un punto obligatorio para las empresas, desarrolladores y todos aquellos responsables del tratamiento de los datos personales.

Para concluir, el RGPD revolucionó a los diferentes sectores y motivo a que las áreas gubernamentales especializadas en protección de datos personales comiencen a incorporar la actualización del marco legal en la agenda. Los estados y organismos deben reflexionar para establecer una norma estandarizada que puede ser aplicable en todo el mundo y para protección de los datos personales de todos los ciudadanos de américa latina.

## Referencias


ADC Digital (2016). El Sistema de protección de datos personales en américa Latina. Oportunidades y desafíos para los derechos humanos. Argentina: ADC Digital. URL: https://adcdigital.org.ar/wp-content/uploads/2017/06/Sistema-proteccion-datos-personales-LatAm.pdf

Agencia de Acceso a la Información Pública de Argentina (2017). Anteproyecto de Ley de Protección de Datos Personales Argentina. Agencia de Acceso a la Información Pública. URL: http://www.jus.gob.ar/media/3223892/anteproyecto_mayo2017.pdf

Alencar, A de S. (2018). ¿En qué consiste la ley general de protección de datos recientemente aprobada en Brasil?. Chile: Derechos Digitales. URL: https://www.derechosdigitales.org/12309/en-que-consiste-la-ley-general-de-proteccion-de-datos-recientemente-aprobada-en-brasil/

Alvarez Rodriguez, L (2015). No uniformidad legislativa: países con legislación en protección de datos personales y sin legislación específica. España: Observatorio Iberoamericano de Protección de Datos. URL:http://oiprodat.com/2015/11/25/no-uniformidad-legislativa-paises-con-legislacion-en-proteccion-de-datos-y-sin-legislacion-especifica/

An, M. (2018). The general data protection regulation is coming. Estados Unidos: Hubspot. URL: https://research.hubspot.com/general-data-protection-regulation?_hstc=259582869.3b6cf65e41c83822b178513ca2285812.1543530714930.1543530714930.1543530714930.1&_hssc=259582869.1.1543530714931&_hsfp=2784807094&_ga=2.219608857.1070284187.1543530709-468980833.1543530709

Bastarrica, D. (2018). Senado aprobó reforma constitucional de protección de datos personales en Chile. Chile: FayerWayer. URL: https://www.fayerwayer.com/2018/05/senado-aprobo-ley-proteccion-datos-personales-chile/

Bertoni, E (2018). Resolución 47/2018. Argentina: Agencia de Acceso a la Información Pública. URL: http://servicios.infoleg.gob.ar/infolegInternet/anexos/310000-314999/312662/norma.htm

Cavoukian, A. (2011). Privacy by design, the 7 foundational principles. Canada: Information and Privacy Commissioner of Ontario. URL: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Diario Oficial de la Unión Europea (2018). Reglamento (UE)2016/679 del parlamento europeo y del consejo. Unión Europea: Diario Oficial de la Unión Europea. URL: https://www.boe.es/doue/2016/119/L00001-00088.pdf

El Reportero (2018). Congreso Nacional aprobó siete artículos más de la Ley de Protección de Datos Personales. Honduras: El Reportero. URL: https://elreportero.hn/?p=7552#.XA3KhnRKjMU

Martinez Molera, L. (2018). El RGPD y sus repercusiones en la industria del Marketing. Hubspot URL: https://blog.hubspot.es/marketing/rgpd-repercusiones-marketing

Presidencia de la República de Brasil. (2018). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasil: Presidência da República Casa Civil Subchefia para Assuntos Jurídicos. URL: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Protección de datos para empresas y autónomos (2018). Derechos Arco: ¿Qué son?. Blog de Protección de datos para empresas y autónomos. URL: https://protecciondatos-lopd.com/empresas/derechos-arco-que-son/#.W_6aZ-hKjMU

Santa Rosa, D. (2018). Desarrollo en materia de protección de datos en Brasil. Estados Unidos: International Association of Privacy Professionals. URL: https://iapp.org/news/a/desarrollos-en-materia-de-proteccion-de-datos-en-brasil/

TYN Magazine (2018). Nueva ley de protección de datos expande la perspectiva commercial en latinoamérica. Argentina: TYN Magazine. URL: http://www.tynmagazine.com/nueva-ley-de-proteccion-de-datos-expande-la-perspectiva-comercial-en-latinoamerica/

Silva P. y Carey G. (2018). Se aprobó en general el Proyecto de ley que modifica la ley de protección de datos en el senado. Chile: Asociación de marketing directo y digital de Chile. URL. http://amddchile.com/se-aprobo-en-general-el-proyecto-de-ley-que-modifica-la-ley-de-proteccion-de-datos-en-el-senado/

Violler, P. (2017). El estado de la protección de datos personales en Chile. Chile: Derechos Digitales. URL: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf