Big data marketing en el MERCOSUR: protección de datos y normas de seguridad

Lic. Bosque, Lía
Universidad Argentina de la Empresa, UADE
Lic. Tondelli, Agustín
Universidad Argentina de la Empresa, UADE.
Mag. Lic. Villan, Marco Antonio
Universidad Argentina de la Empresa, UADE
mvillan@uade.edu.ar

Abstract
"Los objetivos del estudio son analizar la regulación de protección de datos personales y sobre Big Data marketing entre los miembros fundadores del MERCOSUR. Además, se hará hincapié en las normas de seguridad que deben cumplir todos los responsables del tratamiento de datos con fines de mercadotecnia y se comparará con el Reglamento de Protección de Datos de la Unión Europea. Por otro lado, se analizarán la Inteligencia de fuentes abiertas u open source intelligence y la filosofía de los datos abiertos.

Palabras Clave
Privacidad, Seguridad, Big Data Marketing, OSINT, Protección de datos personales

Introducción

En los últimos años el desarrollo de los sistemas informáticos y los grandes almacenes de datos permitieron que el tratamiento de la información sea utilizado para el marketing, por lo que surgió el concepto de Big Data Marketing.
La recopilación de la información y los grandes almacenes de datos que constituyen el Big Data es el eje de debate desde el año 2000 sobre los principales desafíos que giran alrededor de tres dimensiones: el volumen, la velocidad y la variedad. (Laney, 2001).
Hace 10 o 15 años atrás los comportamientos de consumo no eran como los actuales, no porque no exista la tecnología para soportarlo, sino porque los hábitos no eran los mismos. Para la toma de decisiones se tenía que evaluar las alternativas dirigiéndose a los puntos de venta, mediante la búsqueda de información en experiencias de conocidos o por promesas de la publicidad masiva. Post estímulo y con intención de compra, se dirigiría al punto de venta. El packaging, los colores, la marca y otros factores son los que determinarían el producto que seleccionaría el comprador. De esta manera, era muy difícil que las expectativas de los consumidores se encuentren en la experiencia de uso del producto o servicio, esto generaba mayores insatisfacciones.
Actualmente, una vez detectado el deseo, esa necesidad moldeada por la cultura, se evalúan las alternativas disponibles en internet. En la web, que se caracteriza por la densidad y calidad de información, se encuentran desde las características de productos y/o servicios como tal, hasta las calificaciones de la experiencia de uso en base a comentarios y feedback de las personas.
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. Al existir mayor cantidad de datos, la recopilación de datos ocurre desde múltiples fuentes que van desde los teléfonos celulares, la geolocalización, redes sociales, datos públicos y privados, recopilación por radiofrecuencia, domótica y sistemas de la información que involucran datos de individuos. Los dispositivos y tecnologías también involucran datos personales. La seguridad de los datos y la

normativa deben generar un marco de protección para los ciudadanos.
Por otro lado, el caso de Facebook y Cambridge Analytica abrió el debate sobre la necesidad de modificar la regulación y establecer nuevas pautas de seguridad y de privacidad de los datos personales. El incidente de la red social remarcó que datos sensibles fueron expuestos para establecer patrones y predicciones políticas (Cadwalladr y otros, 2018).
A diferencia de la Unión Europea, el MERCOSUR presenta un doble desafío para su regulación: por un lado, la necesidad de actualización de normativas que tienen casi dos décadas de vigencia o más y países que aún no poseen una legislación específica. El 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.
En Argentina, se estima que más del 50% de las empresas desconoce o no logra cumplir con los requerimientos solicitados para cumplir con las regulaciones de privacidad que se exigen en la práctica de marketing. Entre los factores se debe a las dificultados para completar formularios, el desconocimiento y la falta de actualización (AMDIA, 2016).
Durante el artículo se analizará a los cuatro miembros fundadores del MERCOSUR, su regulación, las medidas de seguridad que se exigen a las empresas y el tratamiento específico sobre los datos y el marketing en su formato digital.

Marketing y Big Data

El marketing es la actividad, el conjunto de instituciones y los procesos para crear, comunicar, entregar e intercambiar ofertas que tienen valor para los clientes, socios y la sociedad en general. (American Marketing Association, 2013).
En la actualidad, Big Data y marketing forman un concepto que se basan en la recopilación y análisis de los datos en tiempo real, continua y están basados en la información más actualizada de los consumidores, para poder ofrecerles el producto directamente en su smartphone.
En tanto, Big Data Marketing se puede entender como el proceso de recolección, análisis y ejecución de los insights que fueron deducidos del análisis masivo de datos para mejorar la relación con el cliente, optimizar los resultados de marketing y la medición de la fiabilidad interna de la empresa (Arthur, 2013).
Existen tres tipos de fuentes que pueden recolectarse: los datos recolectados son estructurados, semi estructurados y no estructurados generados por canales tradicionales y digitales. Dentro de las fuentes tradicionales se encuentran las bases de datos y las fuentes digitales el Digital Messaging, email, SMS, mensajes y notificaciones de aplicaciones móviles y publicaciones en las redes sociales (Arthur, 2013).
La mayor cantidad de datos que originan las empresas son del tipo no estructurado, son datos binarios que no tienen una estructura, hasta que posteriormente a través del análisis se puede identificar, procesar y almacenar en forma organizada. Una vez que estos datos son depurados y analizados para captar el público objetivo, se pueden mostrar publicidades en forma objetiva al consumidor de manera personalizada.

Desafíos del Big Data Marketing

Si bien se pueden mencionar los beneficios del Big Data Marketing, el problema ocurre con el tratamiento, la recopilación de la información y su resguardo. Pese a que la International Telecommunications Union (ITU) estableció estándares para la seguridad en Big Data basados en la nube en 2016, la enorme cantidad datos genera la complejidad de llevar a cabo controles

exhaustivos. Además, se introduce el debate de la privacidad porque los datos recopilados que también suelen ser utilizados provienen de fuentes públicas o mismo también desde el seguimiento de los dispositivos o aplicaciones móviles.
Los marketers recolectan información de los clientes, es una forma de mejorar los rendimientos para obtener mayores ganancias. En este sentido las firmas invierten millones en capturar datos. Sin embargo, si bien puede mejorar el rendimiento de la empresa también incrementa los riesgos de vulnerabilidad de los datos y la privacidad. (Martin y otros, 2017)
Otro desafío para el Big Data Marketing es que en el tratamiento de los datos existen diversas vulnerabilidades que van desde accesos indebidos a la información, ataques externos en donde se pueden filtrar datos de clientes y en otros casos la información puede ser utilizada para otros fines los cuáles no fueron recolectados, como el robo de identidad o la publicidad no deseada.

Gobierno abierto y datos

El concepto de Gobierno Abierto surge por los años setenta en Inglaterra, ante la necesidad de demostrar la transparencia gubernamental y fomentar la participación ciudadana. Luego de veinte años, estas ideas comenzaron a tener impacto, que en conjunto con los avances informáticos permiten a la ciudadanía el libre acceso a la información. Las personas pueden conocer las actividades que el gobierno llevo y está llevando a cabo. Estos cambios implican una modernización profunda estatal y está estrechamente ligada al concepto de accountability o rendición de cuentas del gobierno.
La organización que lidera este movimiento es la Open Government Partnership (OGP) que propone que tanto los gobernantes como la sociedad desarrollen planes de acción para que los gobiernos sean más inclusivos, brinden respuestas y rindan cuentas a la sociedad.
El concepto de Gobierno Abierto queda sustentado bajo tres pilares: transparencia, colaboración y participación.
En el MERCOSUR, Uruguay aprobó la Ley de acceso a la información pública en el 2008. Hacia 2012 ya estaba lanzando el primer plan de acción conjunto a la OGP.
Entre los años 2011 y 2013, Brasil impulsó su primer plan de acción, centrándose en demostrar los esfuerzos en mejorar la administración pública y ampliar las redes tecnológicas.
En el caso de Paraguay, en 2015 entró en vigor la Ley 5282/14 “De libre acceso ciudadano a la información pública y transparencia gubernamental”, mediante el decreto parlamentario 4064/15. Fue un gran avance ya que permite que los ciudadanos paraguayos puedan acceder a una oficina de Acceso a la Información Pública y estar adheridos al portal creado en el marco de la normativa.
Por último, Argentina se unió en el año 2012, pero no fue hasta finales de 2015 que se creó la Dirección de Gobierno Abierto de la Subsecretaría de Innovación Pública y Gobierno Abierto de la Secretaría de Gobierno de Modernización, donde realmente se convirtieron en un Gobierno Abierto. En el año 2018 se aprobó la Ley de Acceso a la Información Pública Nº 27.275

Datos abiertos y su utilización para marketing digital

Los datos de Gobierno Abierto son los que se generan dentro de la gestión estatal y puede incluir contrataciones, agencias, gastos e información de empresas del estado. Se pueden saber desde las obras que se llevan a cabo (con presupuestos y licitaciones), o conocer cuáles son los árboles que existen en cada plaza, hasta tener información sobre cuáles son los regalos que le hacen al presidente.
Dentro de los datos que brindan los organismos del estado o planes de infraestructura estatales-privados, podemos conocer información muy útil para las campañas de Marketing Digital. Por

ejemplo, para la industria del turismo, se pueden conocer cuáles son los vuelos, aerolíneas, destinos y aeropuertos con más frecuencia, de esta manera se pueden ver estacionalidades que ayudarían a optimizar los presupuestos.
Hoy en día se puede saber cuáles son los vehículos más patentados, por género, por zona y hasta por color, no solo ayudaría a los mismos fabricantes de autos, sino que podría utilizarse esa información para customizar la venta de accesorios y complementos, o para estimar que zona es en la que más mercado podamos desarrollar.
Otra información recaudada en los planes de infraestructura entre el estado y empresas de telefonía privadas, permiten conocer las zonas de cobertura de wifi o televisión digital, como para definir planes de marketing más eficientes, segmentados por dispositivos y región.

OSINT y marketing

OSINT significa Open Source Intelligence o inteligencia de fuentes abiertas. Es el proceso que se realiza para recabar información de fuentes y datos abiertos con un fin específico. Este análisis puede ser por un lado para rastrear personas, cibercriminales o en el caso del marketing de establecer desde perfiles de consumidores hasta análisis de satisfacción de clientes.
Este proceso se realiza mediante el uso de herramientas específicas, algunas open source y otras de propietarios. Es parte del investigador de discriminar la información no veraz, los resultados duplicados, y debe ser capaz de filtrar los resultados y de elegir los correctos. (Orejón, 2018)
El problema que surge con el análisis de fuentes y datos abiertos con fines de mercadotecnia es que no necesariamente los datos son públicos. Si bien existen datos que los mismos gobiernos publican para fomentar la transparencia de su gestión, puede existir el caso donde las fuentes son ilegales. En estos casos, las empresas si bien utilizarían fuentes abiertas pueden ser datos recolectados ilegalmente donde no se prestó el consentimiento para el tratamiento de la información.

Seguridad y privacidad en Big Data

Todos los sistemas Big Data presentan una arquitectura de clúster que permite escalar. Con un gran número de nodos fuertemente conectados, el mal funcionamiento o el ataque a un número pequeño de unidades puede comprometer al conjunto del sistema. La autenticación de usuarios, tanto personales como de máquina, debe cuidarse especialmente. Esto no ha sido siempre así: existen ejemplos de distribuciones de hadoop que utilizan usuarios sin contraseña para ciertas operaciones entre nodos. (Cloud Security Alliance España, 2015).
El problema de la seguridad y la privacidad es que se encuentra con el dilema de que se debe pensar en otras formas para resguardar datos que están en continuo crecimiento y las formas tradicionales de control pueden ser obsoletas. Se deben tener políticas de control en tiempo real y mantener copias de respaldo activas frente a incidentes de seguridad, así como mantener la calidad de los datos y respetar el ciclo de vida del dato.
En primera instancia hay que comprender la diferencia entre datos personales y datos sensibles. Estos últimos no pueden ser recopilados salvo por excepciones que mencionan las legislaciones regionales e internacionales. En el caso de recopilarlas se deben tener las garantías de los usuarios ya que es información que podría ser utilizada con otros fines y ciberdelitos, se debe proteger la confidencialidad, disponibilidad e integridad de los datos.
En segundo lugar, hay que comprender que el 90% de los usuarios sostienen que tienen la sensación de haber perdido el control de sus datos, que ya no son sus dueños. (IIC, 2016). Esta afirmación podría hacer alusión a la falta de transparencia que existe en las empresas y agencias publicitarias. En este punto surge la necesidad de que el

consentimiento del uso de datos sea claro y conciso para todos los usuarios. El lenguaje claro es fundamental para que los usuarios comprendan los términos y condiciones.
Por último, se deben establecer medidas técnicas y organizativas de seguridad en las agencias de marketing y empresas que realizan tratamiento de datos en cantidades masivas. Las pautas de seguridad que incorporen tienen que incluir tanto el diseño como la gestión de políticas de seguridad y privacidad, el cifrado de datos y la gestión de riesgos entre otros estándares a nivel internacional. También, hay establecer políticas de anonimización y de contingencia frente a incidentes de seguridad para proteger los datos y los datos personales.

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. Las normas 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 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, en la 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.

Legislación actual en el MERCOSUR

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.
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.
En tanto, Uruguay aprobó la Ley N° 18.331, de protección de datos personales, y su decreto parlamentario en 2008. Además, en 2017 se aprobó la Ley Rendición de Cuentas y Balance de Ejecución N° 19.670 que incluye modificaciones a la Ley N° 18331.
En el caso de Paraguay, en 2001 aprobó la Ley N° 1682 que reglamenta la información de carácter privado.
Mientras tanto, Brasil es uno de los países que posee una legislación actualizada que y alineada al reglamento europeo que entró en vigor en 2018.
El análisis también supone que de los miembros fundadores del MERCOSUR, Argentina y Paraguay se encuentran con leyes que se podrían considerar desactualizadas, teniendo en cuenta el desarrollo 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.

Sin embargo, sólo dos países poseen legislación adecuada en América Latina, además de Argentina que posee niveles adecuados de protección de datos desde 2003, en 2012 se incorporó Uruguay. 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.
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.

Seguridad de los datos y el marco legal

En los casos de Argentina, Brasil y Uruguay se establecen criterios similares en cuanto a las medidas de seguridad que las empresas que realizan tratamiento de datos deben cumplir.
Uruguay, en el artículo 10 de la Ley N° 18.331 establece que el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.
Argentina en su Ley N° 25.326 establece en su Artículo N° 9 que el responsable o usuario del archivo de datos debe 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. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.
En Brasil, actualmente se podría considerar uno de los referentes en materia de legislación ya que es el país que posee la legislación más actual y tiene una normativa similar a la de la Unión Europea. Según el capítulo VII de la ley llamado Seguridad y Buenas prácticas, en su artículo N° 46 se menciona que los agentes de tratamiento deben adoptar medidas de seguridad, técnicas y administrativas aptas para proteger los datos personales de accesos no autorizados y de situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o cualquier forma de tratamiento inadecuado o ilícito. En tanto, dice que la autoridad nacional podrá establecer normas técnicas mínimas para que lo establecido en el capítulo mencionado, teniendo en cuenta la naturaleza de la información que se maneja, las características específicas del tratamiento y el estado actual de la tecnología, especialmente en el caso de datos personales sensibles.
Por otro lado, la legislación menciona que, al igual que el Reglamento General de Protección de Datos de la Unión Europea, las medidas de seguridad deberán ser observadas desde el diseño del producto o servicio para su ejecución.
En el caso de Paraguay, la protección de los datos de carácter personal ha dado un paso importantísimo con la promulgación de la Constitución de 1992. En ella se consagran expresamente el derecho a la intimidad, la protección del patrimonio documental y el derecho al acceso a la información. Estás garantías constitucionales no han sido debidamente receptadas por leyes de inferior rango. Tanto la Ley N° 1682 como la N° 1969 han sido promulgadas como paliativos para regular, en alguna manera,

un problema específico en el ámbito financiero: la divulgación de la situación de morosidad de algunos deudores directamente afectados por la actividad de una empresa de informes comerciales confidenciales. Ambas leyes distan mucho de ser los instrumentos normativos necesarios para tutelar en forma adecuada la protección de los datos de carácter personal (Editores Argentina,2010).

Big Data y recopilación de datos con fines publicitarios

Las leyes de Argentina, Uruguay y Paraguay están limitadas en relación con el Big Data. Sin embargo, hay que tener presente que el tratamiento de los datos se puede realizar fuera de dichos territorios y existe una transferencia internacional implícita.
La recopilación de datos es legal siempre y cuando exista el consentimiento por parte de los titulares de los datos. En estos casos podrán ejercer los derechos de acceso y también solicitar un retiro o bloqueo de su nombre de las bases de datos.
Las empresas que realizan Big Data cuentan con una dificultad insalvable para cumplir con la norma. En muchos casos, los datos personales que utilizan para realizar los análisis de Big Data han sido recolectados a lo largo de prolongados períodos de tiempo. Por dicho motivo, no cuentan con el consentimiento de los titulares de los datos o, si lo tienen, el mismo no puede considerarse "informado", ya que no ha contemplado finalidades que hoy en día el Big Data ofrece como alternativas. Esta situación acontece diariamente y se seguirá produciendo con muchas empresas que poseen gran cantidad de datos personales y que aún no han descubierto el potencial económico que los mismos esconden. En muchos casos, ya no se trata de una de falta de previsión al momento de recabar la información sino de una falta de visión a futuro, un futuro que día a día los avances tecnológicos se van encargando de hacerlo más sorprendente (Gandolla, 2015).

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 de 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 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.

Privacidad desde el diseño y por defecto

El concepto de Privacy By Design o privacidad desde el 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 estas (Cavoukian, 2011).
La privacidad desde el diseño fue incorporada en el Reglamento General de Protección de Datos y se agravan las penas para aquellos que no lo cumplan.
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.
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 un especial cuidado con los datos que recopilan de personas menores, para el resguardo se debe contemplar la normativa de cada país donde se tienen los servidores o desde donde se brindan los servicios.

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 N° 78. De esta manera, se debe garantizar la reducción del tratamiento de los datos personales, la seudonomización y dar transparencia a las funciones y al tratamiento, 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.

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.

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 expuestos a publicidad contextual cuando navegan por la web, cuando revisa sus 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)

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 (Martínez 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.

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 a modo de ejemplo la eliminación de los datos de los servidores donde son tratados, de sistemas informáticos propios y de servidores de terceros.
También otro método es la desindexación, por medio del cual se puede solicitar a los buscadores que eliminen la información, con la solicitud del derecho de supresión o el derecho al olvido.
En ese sentido, los responsables del tratamiento de datos deben contar con políticas de destrucción de datos.

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.

Brasil el impulso de los nuevos estándares en el MERCOSUR

El 29 de mayo de 2018, cuatro días después de la entrada en vigor 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. Además, se le prohibirá la recolección de datos y actividades de tratamiento direccionadas en Brasil.
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 han aumentado las sanciones contra aquellos responsables de bases de datos no cumplan la normativa.

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.

Legislación de Brasil y los incidentes de seguridad

El artículo N° 48 de la Ley de Protección de Datos de Brasil menciona que el responsable de las bases de datos deberá comunicar a la autoridad nacional y al titular la ocurrencia de incidente de seguridad que pueda acarrear riesgo o daño relevante a los titulares. Esto supone un avance en la legislación del MERCOSUR. En tal caso en los comunicados de incidentes de seguridad se deberán mencionar la naturaleza de los datos afectados, información sobre los titulares implicados, las medidas técnicas y de seguridad utilizadas para la protección de los datos, los riesgos relacionados con el incidente, los motivos de la demora en el caso que la comunicación no haya sido inmediata y las medidas que se adoptaron o adoptarán para revertir o mitigar los efectos del perjuicio.

Uruguay: ley de rendición de cuentas y cambios en la legislación de protección de datos personales

En octubre de 2018 fue promulgada la Ley de Rendición de cuentas y balance de ejecución presupuestal N° 19.670. En enero de 2019 entró en vigor e incorporó avances en la legislación de protección de datos personales en Uruguay.
La normativa incorpora la tendencia de proteger los datos de los ciudadanos fuera del territorio uruguayo. En el artículo N° 37, dice que regirá también para las actividades del tratamiento en el caso de estar relacionadas con la oferta de bienes y servicios dirigidos a ciudadanos uruguayos o que involucren el análisis de su comportamiento, o si así lo disponen normas de derecho internacional o un contrato.
También, entre las nuevas obligaciones para los responsables y encargados de bases de datos se encuentra el artículo N° 38 que menciona que cuando el responsable de una base de datos o de tratamiento, tome conocimiento de una vulneración a seguridad deberá informar en forma inmediata y de las medidas que adopta a los titulares y a la Unidad Reguladora y de Control de Datos Personales. Se coordinará el curso de acción que corresponda, con el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (CERTuy,2018).

Principio de responsabilidad, privacidad desde el diseño y por defecto en la legislación uruguaya

Le nueva legislación modificó el Artículo N° 12 de la Ley de Protección de Datos Personales N° 18.331, por el artículo N° 39 donde se incorporó el principio de la responsabilidad. De esta manera, tanto el responsable como el encargado de una base de datos son responsables de la violación de las disposiciones de la ley. Además, deberán adoptar las medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales y demostrar su efectiva implementación.

También, sostiene que la reglamentación determinará las medidas que correspondan según los tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización.

Incorporación de la figura del Delegado de Protección de Datos para el tratamiento de datos sensibles y datos masivos en Uruguay.

La Ley N° 19.670 en su artículo N° 40 dice que las entidades públicas, estatales o no estatales, las privadas total o parcialmente de propiedad estatal, así como las entidades privadas que traten datos sensibles como negocio principal y las que realicen el tratamiento de grandes volúmenes de datos deberán designar un delegado de protección de datos.
Entre las funciones que va a tener el delegado de protección de datos, similar a las del data protection officer (DPO) del RGPD, es la de asesorar en la formulación, diseño y aplicación de políticas de protección de datos. También, deberá supervisar el cumplimiento de la normativa sobre dicha protección en su entidad.
En relación con la normativa, deberá proponer todas las medidas pertinentes para adecuarse a los estándares internacionales en materia de protección de datos.
Por último, debe actuar como nexo entre su entidad y la Unidad Reguladora y Control de Datos Personales.

Argentina: Anteproyecto y ley de Protección de Datos Personales en Argentina

En Argentina se encuentra en debate desde el año 2016 el anteproyecto de Ley de protección de datos personales. De esta manera, al igual que Brasil y Uruguay se busca actualizar la Ley 25.326 y alinearse a la normativa de la Unión Europea (Agencia de Acceso a la Información Pública, 2017).
Entre los aspectos destacados del anteproyecto es la creación de la figura del delegado de protección de datos personales, la inclusión de la obligación de la privacidad desde el diseño y por defecto, También, propone regular en carácter especial los datos personales de niños, niñas y adolescentes.

Medidas seguridad para el tratamiento y conservación de los datos personales en medios informatizados y criterios para mejores prácticas en la legislación argentina

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.
Por otro lado, en enero de 2019 la Agencia de Acceso a la Información Pública aprobó los criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley N° 25.326.
Se puede destacar el criterio que trata sobre el tratamiento de datos de niños, niñas y adolescentes. Hay que tener en cuenta que las personas utilizan celulares y aplicaciones desde muy jóvenes y se ven impactados por la publicidad y la creación de perfiles. Las buenas prácticas estarían relacionadas al consentimiento del menor: si la persona es menor de edad y no posee la capacidad suficiente para prestar el consentimiento informado, el titular de la responsabilidad parental o tutela sobre la niña, niño o adolescente deberá prestar el consentimiento para el tratamiento de sus datos personales. En tal caso, el responsable de la base de datos deberá realizar esfuerzos razonables para verificar que el consentimiento haya sido efectivamente otorgado por el titular de la responsabilidad parental o tutela sobre el menor de edad, teniendo en cuenta sus posibilidades para hacerlo. (Bertoni,2019).

Aspectos problemáticos del anteproyecto argentino: datos sensibles, Big Data, consentimiento y publicidad

Del análisis del anteproyecto surgen cuestiones que podrían afectar a los objetivos de la Ley.
Entre los problemas más destacados se puede mencionar que no hay una incorporación de los datos biométricos y genéticos como datos sensibles. En el RGPD se encuentran incorporados en el artículo N° 9.
En relación con el consentimiento, tratado en el Artículo N° 12 establece que el tratamiento de los datos personales requiere del consentimiento libre e informado de su titular para una o varias finalidades específicas. Sin embargo, luego establece que el consentimiento se puede obtener de forma expresa o tácita (Fundación Vía Libre, 2018).
En materia de publicidad, el artículo N° 68 puede beneficiar a todas aquellas personas físicas o jurídicas que realizan campañas publicitarias mediante medios electrónicos, pero también es un punto que podría habilitar a realizar envío de correos masivos. El anteproyecto menciona que las pueden tratarse sin consentimiento de su titular datos personales con fines de publicidad, venta directa y otras actividades análogas, cuando estén destinados a la formación de perfiles determinados o que permitan establecer hábitos de consumo que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios. En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, internet u otro medio que permita la tecnología en el futuro, el responsable o encargado del tratamiento debe implementar medidas razonables que informen al titular de los datos la posibilidad de ejercer los derechos de acceso sin cargo ni limitación temporal.
El mismo artículo también destaca que los datos referentes a la salud sólo pueden ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la Ley siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro.
Otro artículo que podría diferir del Reglamento Europeo es el N° 32, acerca de las valoraciones personales automatizadas. El titular de los datos tiene derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa. Sin embargo, no incluye la valoración sea realizada por personas como es el caso del RGPD, sino únicamente por máquinas.

Paraguay y su legislación

Paraguay cuenta con fuerte protección constitucional a la intimidad y la inviolabilidad de la comunicación de las personas, así como el derecho a la autodeterminación informativa. Además, tiene varias normativas que abarcan de forma dispersa el tratamiento de datos personales, la recolección y su uso. (TEDIC, 2017)
Sin embargo, es necesaria una normativa integral para regular los posibles abusos con los datos personales tanto en el sector público como en el sector privado. La regulación es sectorial, pero se necesita un debate global para establecer estándares adecuados al Reglamento General de Protección de Datos Personales de la Unión Europea.

Conclusión

Las normas de seguridad que deben cumplir las empresas que realizan Big Data Marketing deben ser medidas que puedan resguardar la confidencialidad y la privacidad de los datos personales. Deben tener niveles básicos, medios y avanzados que permitan asegurar que los datos no caigan en manos de terceros.
Sin embargo, el desafío para las empresas de marketing de Latinoamérica es muy amplio porque por un lado debe adaptar sus políticas de privacidad y seguridad a la normativa Europa si realizan el tratamiento de datos de ciudadanos europeos, por otro es estudiar y analizar las políticas de seguridad de la región y por último invertir en medidas de seguridad robustas que puedan brindar las medidas técnicas y organizativas que exigen las leyes del MERCOSUR.
Por último, hay que reflexionar acerca del estado actual del marco legal de la región y la necesidad trabajar en un esfuerzo conjunto en la creación de una normativa unificada y también hacer hincapié en exigir mayores medidas de seguridad.

Referencias

[1]Acuña J., Fulchi Luis A., Sequera M. (2017). La Protección de datos personales en bases de datos públicas en Paraguay. Paraguay: Tecnología y ComunidadURL:https://www.tedic.org/wp-content/uploads/2017/09/La-protecci%C3%B3n-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf

[2] 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

[3] 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

[4]Agencia de Acceso a la Información Pública (2018). Ley de Protección de Datos Personales. Argentina: AAIP. URL:https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf

[5] 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/

[6] 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/

[7] 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

[8] Arthur, L. (2013). Big Data Marketing. New Jersey, EUA: WILEY

[9] AMA. (2013). Definitions of marketing. Estados Unidos: American Marketing Association. URL: https://www.ama.org/the-definition-of-marketing/

[10]AMDIA (2016). Nuevas perspectivas de protección de datos personales en la Argentina. Argentina: AMDIA. URL: http://amdia.org.ar/site/nuevas-perspectivas-de-proteccion-de-datos-personales-en-la-argentina/

[11] Balaguero, T (2018). Big Data: la seguridad de los datos. España: Deusto Formación. URL: https://www.deustoformacion.com/blog/blog-empresa-nuevas-tecnologias/big-data-seguridad-datos

[12]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

[13]Cadwalladr C. y Graham-Harrison E.(2018). How Facebook Cambridge Analytyca turned facebook likes into a lucrative political tool. Reino Unido: The Guardian. URL: https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

[14]Cloud Security Alliance España (2015). Implicaciones de seguridad de Big Data. España: CSAES. URL: https://www.ismsforum.es/ficheros/descargas/implicaciones-de-seguridad-de-big-data1448462176.pdf

[15]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

[16]Corrales M. y Piera A. (2010). Protección de datos de carácter personal: el Paraguay dentro del marco económico-legal del MERCOSUR. Argentina: IJ Editores Argentina. URL:

https://ar.ijeditores.com/articulos.php?idarticulo=62107&print=1

[17]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

[18]Escuela de Alta Dirección Pública (2017). Estado Abierto, revista sobre el estado, la administración y las políticas públicas. Argentina: INAP URL:https://www.argentina.gob.ar/sites/default/files/estado_abierto_1_2.pdf

[19]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

Fundación Vía Libre (2018). Proyecto de Ley de (Des)Protección de Datos Personales. Argentina:

[20]Fundación Via Libre. URL:https://www.vialibre.org.ar/wp-content/uploads/2018/10/Comentarios.Proyecto.147-2018.pdf

[21]Gandolla, L. (2015) Conflictos entre big data y la ley de protección de datos personales. Argentina: SAIJ. URL: http://www.saij.gob.ar/doctrina/nv13417-gandolla-conflictos_entre_big_data.htm

[22]IIC (2016). Seguridad en Big Data, privacidad y Protección de datos. España: Instituto de Ingeniería de Conocimiento. URL: http://www.iic.uam.es/innovacion/seguridad-big-data/

[23]Infonegocios (2017). La Protección de datos personales en bases de datos públicas en Paraguay. Paraguay: Infonegocios. URL:http://www.infonegocios.com.py/infotecnologia/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay

[24]Instituto Latinoamericano y del Caribe de Planificación Económica y Social. (2012). Datos abiertos: un nuevo para los gobiernos de la región. Chile: CEPAL URL:https://www.cepal.org/ilpes/noticias/paginas/3/54303/Datos_Abiertos_Un_Nuevo_Desafio_Gobiernos.pdf

[25]Laney, D. (6 de febrero de 2001). 3D Data Management: Controlling Data Volume, Velocity and Variety. 3D Data Management: Controlling Data Volume, Velocity and Variety. Stamford: META Group Inc.

[26]Martin K, and Murphy, P. (2016) The role of data privacy in marketing. URL: https://www.researchgate.net/publication/308578866_The_Role_of_Data_Privacy_in_Marketing

[27]Martin, K, Borah, A y Palmatier R.(2017). How Should Marketers Manage Data Privacy?. Estados Unidos. Association Marketing Association. URL: https://www.ama.org/2017/11/01/how-should-marketers-manage-data-privacy/

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

[29]MAS, A. (2016). ¿Cómo es la seguridad en la era de Big Data?. Argentina: MassNegocios. URL: http://www.iic.uam.es/innovacion/seguridad-big-data/

[30]Orejon,S (2018). OSINT o cómo pescar en la red. España: INESDI. URL: https://www.inesdi.com/blog/osint-pescar-red/

[31]Open Government Partnership (2017). Cómo Paraguay abrió 27 oficinas de acceso a la información pública en tan solo 10 días. Estados Unidos: OGP URL:https://www.opengovpartnership.org/stories/c-mo-paraguay-abri-27-oficinas-de-acceso-la-informaci-n-p-blica-en-tan-solo-10-d

[32]Parlamento Uruguayo (2017). Rendición de Cuentas y Balance de Ejecución Presupuestal. Uruguay: Parlamento. URL:https://legislativo.parlamento.gub.uy/htmlstat/pl/leyes/Ley19670.pdf

[33]Parlamentario (2018). Crearon la Agencia de Acceso a la Información Pública. Argentina: Parlamentario. URL:http://www.parlamentario.com/noticia-107567.html

[34]Piscitelli, E. (2018). OSINT: open source intelligence aplicacion a las investigaciones. Argentina: OSINT Latam Group. URL:https://osintlatamgroup.com/2018/12/osint-open-source-intelligence-aplicado-a-las-investigaciones/

[35]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

[36]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

[37]Roy, M (2016). Big Data Security, privacy becomes a concern for marketing analytics. URL: https://searchcompliance.techtarget.com/feature/Big-data-security-privacy-becomes-a-concern-for-marketing-analytics

[38]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/

[39]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/
[40]Unidad Reguladora y Control de Datos Personales (2017). Cambios recientes a la legislación sobre protección de datos personales. Uruguay: Sitio Oficial de la República Oriental del Uruguay URL:https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/cambios-recientes-legislacion-sobre-proteccion-de-datos-personales-en

Contacto:mvillan@uade.edu.ar, lbosque@uade.edu.ar, atondelli@uade.edu.ar