PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA:

LO BUENO, LO MALO Y LO MEJORABLE

accessnow.org

accessnow

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación del apoyo técnico directo, el análisis integral de políticas públicas, la incidencia global, la entrega de subvenciones para grupos locales emergentes, y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

accessnow

PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA:

LO BUENO, LO MALO Y LO MEJORABLE

La Agencia de Acceso a la Información Pública de Argentina, órgano encargado de la aplicación de la Ley de Protección de Datos Personales, elaboró durante 2017 un anteproyecto de ley para la actualización de la normativa sobre la materia siguiendo el ejemplo de la Unión Europea. En agosto de 2018, el presidente argentino, Mauricio Macri, anunció que enviaría al Congreso Nacional el anteproyecto en cuestión, en cuya última versión basamos el siguiente análisis.

La reforma se produce en el marco de la implementación desde el 25 de mayo de 2018 del Reglamento General de Protección de Datos de la Unión Europea (GDPR por sus siglas en inglés) aprobado en abril de 2016. En Access Now creamos un informe con recomendaciones para un marco legal de protección de datos basados en la experiencia de la GDPR. En general, el anteproyecto de ley argentino sigue el lineamiento de la nueva norma europea en varios aspectos. La GDPR sirve de ejemplo para muchos países, producto de su extensa y participativa elaboración. Sin embargo tanto la norma europea como el anteproyecto argentino, no están exentas de desaciertos.

A continuación analizaremos lo bueno, lo malo y lo mejorable del anteproyecto argentino de reforma de la ley de protección de datos personales.

LO BUENO

1) El anteproyecto incluye definiciones claras que, aunque no son tan precisas como las de la norma europea, establecen los conceptos más importantes. (Art. 2).

2) El anteproyecto enuncia principios fundamentales para una correcta protección de los datos personales: principio de licitud, lealtad y transparencia; principio de finalidad; principio de minimización de datos; principio de exactitud; limitación del plazo de conservación; principio de responsabilidad proactiva; principio de seguridad de los datos personales; principio de confidencialidad. Puede leer más acerca de estos principios en nuestra **guía** sobre la protección de datos.

3) Toda ley de protección de datos debe establecer claramente los casos en los cuales los datos pueden ser procesados. En esto el anteproyecto de ley cumple, al igual que la norma europea. Sin embargo, hay dos casos que requieren mayor cuidado: la autorización del procesamiento de los datos para la satisfacción de un "interés legítimo" y cuando el tratamiento de los datos se refiera a los que figuren en "fuentes de acceso público irrestricto". Desarrollaremos cada uno de estos casos posteriormente.

4) La reforma incluye una amplia lista de derechos de los usuarios similar a la de la reglamentación europea: derecho de acceder a la propia información de forma clara y comprensible, derecho a rectificar los datos, derecho a oponerse a su tratamiento, derecho a solicitar la supresión de los mismos, derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos y derecho a transferir los datos de una plataforma a otra que ofrezca similares servicios. Estos derechos son clave para que cada usuario permanezca en control de su información.

5) En el artículo 4, el anteproyecto de ley describe su ámbito de aplicación y plasma el principio de extraterritorialidad, el cual permite brindar una suficiente protección de los datos personales y de los derechos de los usuarios que estén en Argentina, aún cuando el responsable de su tratamiento se encuentre en el extranjero.

A pesar de ello, la implementación de este principio podría traer algunas complicaciones: conflictos de jurisdicción, es decir, que dos o más jueces o tribunales de distintas naciones entiendan que tienen facultades para dirimir sobre un mismo asunto; conflicto de leyes, cuando dos o más normas de distintos países son aplicables para el mismo caso; etc. Para evitar estas situaciones es necesario que los legisladores indiquen claramente los casos en los que las leyes resulten aplicables fuera del territorio, a qué sujetos específicamente, y los mecanismos a utilizar para la ejecución de las decisiones judiciales.

6) A medida que cada país sancione leyes siguiendo los lineamientos de la GDPR, los datos personales estarán debidamente protegidos cuando existan transferencias internacionales. Mientras tanto, es importante crear mecanismos seguros para la transmisión de datos a terceros países. Es necesario establecer pautas estrictas y sistemas transparentes de control e incluir recursos eficientes que aseguren que los derechos de los usuarios viajen junto a su información. El capítulo 5 de la GDPR (arts. 44 a 50), por ejemplo, establece mecanismos para la transmisión de datos como la determinación de la adecuación de terceros países respecto de las garantías mínimas para la protección de datos. El objetivo de esta evaluación es permitir la transferencia internacional sólo a países con niveles

de protección adecuados. Otros mecanismos de transmisión de datos como cláusulas contractuales específicas entre empresas o contratos entre entidades perteneciendo al mismo sector comercial también existen bajo la GDPR.

El anteproyecto de ley argentino ha ampliado y actualizado la regulación. Aunque en menor extensión si se compara con la GDPR, ha brindado las condiciones necesarias para proteger el intercambio de datos tanto con otros países como con servicios de tratamiento de datos personales por medios tecnológicos tercerizados.

7) A medida que aumenta el número de usuarios de servicios en línea, se hace cada vez más importante brindar seguridad a los datos personales y a la privacidad. Para lograr esto es fundamental que durante la fase de diseño de productos y servicios se desarrollen e implementen medidas tecnológicas y organizacionales apropiadas. Tanto la GDPR como el Proyecto argentino regulan la "protección de datos desde el diseño y por defecto" en normas prácticamente idénticas (art. 25 y art. 38 respectivamente), y de ese modo contribuyen a la seguridad e integridad de la información.

8) Los datos personales se pueden filtrar a pesar de que existan medidas de seguridad y correcto tratamiento de datos. Es fundamental en estas situaciones adoptar mecanismos de prevención y notificación a los usuarios. La norma europea y el anteproyecto de reforma de la ley argentina contienen disposiciones relativas a la notificación en caso de incidentes de seguridad. En el caso de la propuesta de ley argentina, esas comunicaciones deben remitirse a la autoridad de aplicación. En casos graves, también a los titulares de los datos (art. 20).

9) Para implementar eficientemente las leyes de protección de datos personales es necesario crear autoridades de control independientes y mecanismos coercitivos robustos. Para cumplir con el primer requisito el anteproyecto de ley le brinda la función de autoridad de control a la Agencia Nacional de Protección de Datos Personales (ANPDP), ente descentralizado con autarquía económica y financiera. Las sanciones también aumentan en comparación con la existente ley de datos personales. Sin embargo en estos dos puntos hay que realizar salvedades, ya que las sanciones no suelen cumplirse en su totalidad. Este tema será tratado con posterioridad.

10) En estas leyes, es común confundir el derecho a eliminación de los datos con el derecho al olvido. Mientras que el primero permite a los usuarios pedir que se borre su información cuando dejan de usar un servicio o producto; el derecho al olvido implica obligar a terceros a esconder información referida al titular de los datos cuando esta deja de ser relevante o queda desactualizada.

Respecto del derecho al olvido, **ya hemos dicho** que su existencia genera un riesgo de eliminación excesiva de información y por lo tanto, podría ser usado como mecanismo de censura. Además, poner a intermediarios de información en la posición de decisores sobre la relevancia de la información y el interés público con el que debiera equilibrarse, genera un problema de legitimidad y un incentivo peligroso para los sujetos involucrados.

Es por ello que se desaconseja la implementación de este derecho. La propuesta de modificación de la ley argentina correctamente evita confundir estos derechos y no reconoce un "derecho al olvido", alejándose así de la GDPR europea. Para más información, lea nuestro

análisis sobre la aplicación global del **derecho al olvido** que detalla los riesgos en su aplicación y recomienda protecciones adicionales para su implementación en la Unión Europea.

11) Desde Access Now, recomendamos contar con un proceso de revisión continuo de la aplicación de las leyes de protección de datos. Constantemente surgen nuevos desafíos en materia de protección de datos personales, por lo que se hace difícil contar con una ley completamente actualizada o a prueba de lo que pueda suceder en el futuro. Es por ello que la actualización de la norma argentina es una buena noticia. De todos modos, es importante comprender que estas leyes deben ser flexibles en su aplicación y adaptarse a tecnologías y prácticas sociales que están en cambio permanente.

12) A menudo las empresas responsables del procesamiento de datos tienden a adoptar sus propias medidas de seguridad de la información. Si bien esta actitud es loable, es fundamental que las leyes de protección de datos brinden un marco para desarrollar estándares mínimos de seguridad. Las recomendaciones de buenas prácticas por parte de los organismos de aplicación también juegan un papel importante en esto. De esta forma se evita que los métodos adoptados sean insuficientes, contradictorios y excesivamente flexibles, lo que puede perjudicar el cumplimiento de las obligaciones de protección por parte de las empresas.

Tanto la GDPR como el anteproyecto de ley argentino crean un claro marco regulatorio para las organizaciones, lo que permite un desarrollo de productos y servicios compatible con derechos fundamentales.

LO MALO

1) Es fundamental que todos los interesados en la ley puedan participar y opinar en forma abierta y transparente junto a los encargados de elaborarla y sancionarla. En el caso del anteproyecto argentino se realizaron consultas a la comunidad y a especialistas, lo que llevó a la modificación del primer borrador. Sin embargo, hay aspectos que no se tuvieron en cuenta para mejorar la inclusión, publicidad y transparencia del proceso. En primer lugar, no conocemos la injerencia que tuvieron o tienen los distintos interesados en la ley (lobbistas). En segundo lugar, la participación de especialistas y organizaciones civiles fue escueta y generalmente circunscrita al ámbito de la ciudad de Buenos Aires.

2) Los gobiernos tienen la obligación de proteger los datos personales, incluso cuando esa información se encuentra en manos de organismos del Estado. Pese a ello, suelen establecerse limitaciones y excepciones a la protección de datos respecto de ciertas actividades gubernamentales, frecuentemente aduciendo necesidades prácticas o la protección de otros intereses en pugna. La GDPR contiene una lista de 10 causales por las cuales los Estados miembros pueden limitar los derechos de los usuarios (art. 23). La vaguedad del lenguaje utilizado, a menudo incorporado adrede, es criticable. Suele usarse para cubrir un amplio rango de actividades estatales con límites poco definidos en la práctica como "la seguridad nacional".

El anteproyecto de ley argentino dispone que puede negarse el ejercicio de los derechos en función de "la protección de la defensa de la Nación, del orden y la seguridad públicos, o de

la protección de los derechos e intereses de terceros" (art. 36). Estas excepciones no sólo son más amplias y menos definidas que las de la norma europea, sino que pueden acarrear consecuencias más graves producto de la interpretación excesiva de las normas de seguridad nacional que los gobiernos latinoamericanos suelen sostener.

Es por ello que recomendamos limitar y esclarecer este tipo de excepciones y promover su uso sólo cuando sean necesarias y proporcionadas, incluyendo la supervisión de la autoridad de aplicación y la existencia de mecanismos accesibles de recurso y reparación.

3) Las compañías frecuentemente argumentan que tienen un interés legítimo que habilita a recolectar y procesar información personal sin necesidad de notificar a los usuarios. La GDPR recepta esta justificación en su artículo 6, inc. 1, f. El anteproyecto de ley argentino también lo hace y dispone que "el tratamiento de datos es lícito sólo si se cumple al menos UNA (1) de las siguientes condiciones:...g) el tratamiento de datos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente." (art. 11, inc. g).

Esta última salvedad, si bien es importante a los fines de limitar la excepción, no es suficiente. En la forma en la que está redactado el artículo, las compañías serán quienes evalúen los derechos en juego, lo que puede llevarlas a efectuar el tratamiento de datos manteniendo a los usuarios en desconocimiento de esta actividad. Creemos que esto contradice el objetivo de la protección normativa, en particular respecto de grandes empresas, ya que reduce las posibilidades de control de los usuarios sobre su información. Cláusulas de autorización basadas en el mero interés como estas deberían complementarse solicitando al menos un requisito más que refuerce el conocimiento y participación efectivas del titular de los datos.

4) Al regular el tratamiento de datos sensibles –aquellos que hacen referencia al origen racial o étnico, opiniones políticas, religión, estado de salud, sexualidad, etc.– la ley debe ser particularmente estricta y establecer una limitación general, con excepciones limitadas y claras. La norma europea autoriza la recolección y procesamiento de esta información sin consentimiento expreso del titular cuando sea con la finalidad de realizar investigaciones científicas o históricas o con fines estadísticos (art. 9 inc. 2, j). Esta disposición ha sido criticada por ser una excepción demasiado amplia y potencialmente peligrosa en el contexto del crecimiento de la industria de la e-salud, la internet de las cosas y el análisis de big data para fines políticos.

Luego de una insistente lucha por parte de organizaciones civiles, incluida Access Now, se logró incorporar a la GDPR la salvedad "con fines en el interés público" lo cual limita al uso discrecional de esta justificación para procesar datos sensibles.

Esta excepción también se encuentra incluída en el anteproyecto de ley argentino (art. 16, inc. f). No incluye la limitación de tener por finalidad el interés público pero tiene como agregado el requisito de adoptar un procedimiento de disociación de datos (de manera que la información no pueda asociarse a una persona determinada). Estos métodos pueden brindar mayor seguridad al titular de los datos al mantenerlo en el anonimato,

sin embargo, **se ha discutido la efectividad de estos procedimientos**. Lo correcto para los casos de duda es requerir siempre el consentimiento libre, informado y revocable. Adicionalmente, ya que el anteproyecto sigue los lineamientos generales de la GDPR, sería importante incluir la finalidad de "interés público" para autorizar el tratamiento de información sensible sin consentimiento de los titulares.

5) Para el caso de filtraciones de información, es necesario adoptar mecanismos de prevención y notificación que incluyan a los usuarios. Lo malo en la regulación de esta cuestión tanto en la norma europea como en el anteproyecto de ley argentino es que dejan a discreción de las compañías si corresponde o no notificar a los usuarios. La comunicación a los usuarios se considera necesaria sólo "cuando sea probable que entrañe altos riesgos a sus derechos". Este agregado otorga un excesivo margen de actuación a las empresas. Es necesario definir de forma clara y estricta cuales serían los casos de "alto riesgo", aunque sería ideal la eliminación de esta frase y por lo tanto, la notificación de incidentes considerados a priori menos graves.

6) Ya hemos mencionado la necesidad de contar con una autoridad de control independiente. El anteproyecto de reforma de la ley argentina dispone en su artículo 62 que la autoridad de control será "dirigida, administrada y representada por un director ejecutivo designado por el término de cuatro (4) años, por el poder ejecutivo nacional con posibilidad de ser reelegido por una única vez.".

Tanto la duración del cargo como la posibilidad de reelección coinciden con los términos del mandato presidencial en Argentina. Además, el director de la autoridad de aplicación es nombrado por el poder ejecutivo. Esto puede traer la indeseable consecuencia de la designación de un director que se ajuste a las políticas del gobierno de turno. Se recomienda, por lo tanto, la intervención del poder legislativo para la designación del director. Esto mejoraría la independencia de la autoridad de aplicación y guardaría coherencia con el procedimiento de remoción, que prevé la intervención de una "comisión bicameral del Honorable Congreso de la Nación" (artículo 65).

7) Para el correcto cumplimiento de la ley, se hacen necesarias sanciones duras y efectivas para los casos de violación a sus disposiciones. En Europa, antes de la sanción de la GDPR, las multas eran considerablemente bajas (150.000Đ) por lo que muchas compañías no cumplían con la ley de protección de datos personales ya que su cumplimiento resultaba más oneroso que el pago de las sanciones. Es por ello que la nueva norma europea dispuso multas de "una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior…".

El anteproyecto de ley argentino establece como sanción en el artículo 76 inc. b) una "multa que podrá alcanzar el equivalente a quinientos (500) salarios mínimos vigentes al momento de la imposición de la sanción". Para el caso de grandes empresas que manejan datos personales en la Argentina, esta suma máxima podría resultar escasa. De este modo, de acuerdo a la gravedad de la falta, podría resultar más conveniente pagar la multa que cumplir la ley.

LO MEJORABLE

En este apartado nos tomamos la licencia de hacer algunas críticas y sugerencias a partir de las diferencias entre el anteproyecto de reforma de la ley de protección de datos argentina y la GDPR europea.

1) La utilización de la técnica de disociación de datos en el caso del tratamiento de datos sensibles puede resultar insuficiente. Un error frecuente es pensar que anonimización de datos son siempre efectivos y por lo tanto, suficientes para la protección de los datos personales. Se han documentado **técnicas de "data mining"** (procesamiento de grande bases de datos pre-existentes con el fin de generar nueva información) con las que información anonimizada es entrecruzada con otras fuentes de información permitiendo re-identificar a los titulares de los datos.

Es por ello que se hace fundamental una correcta reglamentación, o en mejor medida, una regulación de mayores requisitos para el procesamiento de datos sensibles. En esto la actuación del organismo de aplicación y su liderazgo técnico serán de vital importancia.

2) El anteproyecto de ley argentino define su campo de aplicación en el artículo 2, mencionando a las "fuentes de acceso público irrestricto" y las "fuentes de acceso público restricto". Estos conceptos no están en la GDPR. Poseen una gran relevancia en el anteproyecto de reforma de la ley porque las fuentes de acceso público irrestricto se presentan como una excepción a la obtención del consentimiento para la licitud en el tratamiento de datos.

La discusión recae sobre el concepto de "fuente de acceso público irrestricto". Según su definición actual, mucha información que se encuentra accesible al público en internet se encontraría comprendida. Es el caso de los contenidos "públicos" de plataformas como Facebook y Twitter, entre otras. De ser así, el tratamiento de estos datos sin necesidad de obtener el consentimiento de sus titulares iría claramente en contra del espíritu general de la ley al perder los usuarios el control sobre la recolección y tratamiento masivos de su información.

3) El artículo 3 del anteproyecto de reforma excluye del ámbito de la ley al "tratamiento de datos que realicen los medios de comunicación en el ejercicio de la libertad de expresión". Siendo que nos encontramos ante un caso tan extremo como es la absoluta inaplicabilidad de la ley, sería importante definir más claramente cuáles serían los casos en los que los medios de comunicación estarían exceptuados. Esto es importante para el caso de medios de comunicación convergente, algunos cuasi monopólicos, que integran actividades económicas muy variadas y manejan enormes cantidades de datos de sus usuarios y consumidores. Además, para proteger el anonimato y seguridad de las fuentes, sería necesario que algunas medidas de protección de datos personales y en particular de seguridad de la información se apliquen a las áreas de los medios que custodian información importante.Consideramos que al menos sería importante dar una amplia participación a distintos sectores sociales, especialistas y organizaciones civiles a los fines de determinar si es este el mejor camino o si el caso amerita una regulación específica.

4) El artículo 59 del anteproyecto argentino regula el tratamiento de datos por parte de los organismos de seguridad e inteligencia. La norma dispone que "El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia, cuando sea necesario realizar sin el consentimiento del titular, queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos". A pesar de las importantes limitaciones sobre el uso de datos que establece la norma, aconsejamos la inclusión de requisitos de derechos humanos para el tratamiento. Entre ellos, podemos mencionar los requisitos de necesidad, proporcionalidad y de autorización legal previa para la conducta de estas prácticas en acuerdo con **principios internacionales** en la materia.

5) La norma de protección de datos europea incluyó un sistema de códigos de conducta y de certificados para que las empresas se ajusten a la nueva normativa. Consideramos que este sistema o uno similar sería de utilidad en la reforma argentina, ya sea incorporándolo en el cuerpo de la ley o en su norma reglamentaria.

De seguirse esta recomendación sería importante controlar la implementación de los códigos de conducta y certificados para evitar que las empresas hagan abuso de ellos considerándolos condición suficiente para a transferencia de datos a países con niveles de protección insuficientes.

6) En el anteproyecto, las compañías pueden procesar datos basándose en un "interés legítimo" sin necesidad de obtener el consentimiento de los titulares de los datos ni de comunicarle dicho tratamiento. Esta cuestión fue ampliamente cuestionada en las tratativas previas a la GDPR sin un resultado exitoso.

Creemos que una solución para evitar abusos sería crear una "obligación de comunicación previa al tratamiento de datos". Esto sería coherente con el art. 11 inc. g el que autoriza el tratamiento basado en el interés legítimo del responsable "siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente". De no existir al menos una comunicación obligatoria, los usuarios no lograrían tomar conocimiento de que sus datos están siendo procesados y no podrían ejercer sus derechos. Esto implicaría una prevalencia de los intereses de las compañías sobre los intereses de los usuarios.

7) En el año 2016 el gobierno argentino, particularmente la Jefatura de Gabinete nacional, hizo **uso de los datos personales de ciudadanos registrados en la Administración Nacional de Seguridad Social (ANSES) para comunicaciones oficiales del gobierno.** Esta situación excesiva y lesiva de derechos fue justificada en lo dispuesto por el artículo 5 inc. b de la ley vigente, el cual dispone la licitud del tratamiento sin necesidad de consentimiento cuando los datos "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal". Esta misma excepción, con distintas palabras, se encuentra en el anteproyecto de ley en el artículo 11 inc. c. Creemos que es necesario incluir límites expresos a esta facultad discrecional del Estado, estableciendo requisitos y limitaciones más específicos.

CONCLUSIÓN

El avance de las comunicaciones y la tecnología hacen necesaria la modernización y adaptación de las leyes, sobre todo cuando esos avances pueden afectar derechos fundamentales. En materia de datos personales, la GDPR se ha convertido en una importante guía para todos los países que quieran modernizar sus leyes a los fines de brindar una correcta protección. Sin embargo, cada región y cada país tienen particularidades que deben ser tomadas en cuenta.

Esto implica que los elementos positivos de la legislación de vanguardia extranjera pueden ser incorporados a las legislaciones locales. Pero que debe evitarse una traslación irreflexiva de soluciones jurídicas a un ámbito con desafíos propios y realidades diferentes. Tanto Argentina como toda Latinoamérica presentan realidades muy distintas a las de Europa que no podemos dejar de lado. El caso del derecho al olvido es uno de los ejemplos más claros, en función de los desafíos para el acceso a la información pública y en relación a las reivindicaciones históricas que siguen vigentes en varios países de la región.

En las **Lecciones del Reglamento General de Protección de Datos de la UE** dejamos en claro que la GDPR tiene importantes puntos débiles criticados por académicos y la sociedad civil. Por lo tanto, es necesario que cada país realice un debate amplio y participativo a través de sus congresos y en conjunto con especialistas, representantes de la sociedad civil y empresas, con el objetivo de brindar una protección adecuada a los derechos de los usuarios locales.

Creemos que en el caso del anteproyecto argentino se logró un buen equilibrio, adoptando soluciones útiles y evitando las problemáticas. Desde Access Now celebramos la iniciativa de la Agencia de Acceso a la Información Pública, ente coordinador del anteproyecto que analizamos. Y nos ponemos a disposición para colaborar en el proceso de discusión de la ley en el Congreso argentino para construir un marco regulatorio que garantice la debida protección de los derechos digitales.

Este documento es una publicación de Access Now. Para más información, por favor visite: **https://www.accessnow.org**

AUTOR
Gaspar Pisanu, (pasante de políticas públicas)

COLABORACIÓN Y EDICIÓN
Javier Pallero (coordinador de políticas públicas para América Latina)
Estelle Massé (analista senior de políticas públicas para Europa)
Juliana Castro (asociada de diseño, Nueva York)

DISEÑO GRÁFICO
Juliana Castro (asociada de diseño, Nueva York)