Requisitos mínimos para la Reforma de la Ley de Protección de Datos Personales de Argentina

Este documento presenta un conjunto de reflexiones desarrolladas por las organizaciones y los y las profesionales abajo firmantes, especializadas en el ámbito de los derechos humanos, en el entorno digital orientadas a alimentar el debate en torno a la normativa de protección de datos personales en Argentina. Se centran en los mínimos necesarios que, con base en nuestra experiencia, debe comprender dicho proyecto de reforma con el objeto de satisfacer estándares adecuados de protección alineados con el respeto de los derechos humanos consagrados en la Constitución y en tratados internacionales ratificados por Argentina. Seguramente, este documento será profundizado por las organizaciones y profesionales firmantes -de manera individual o conjunta- en futuras instancias de participación y consulta establecidas para el proceso de reforma.

La demanda por una legislación integral y moderna de protección de datos personales se relaciona con la necesidad de promover la confianza y la certeza jurídica en el uso de datos como base de la economía y la innovación en la sociedad de la información. Asimismo, es requerida como garantía para la autodeterminación de las personas, lo que contribuye a fortalecer y consolidar la democracia y los regímenes basados en el reconocimiento de los derechos humanos.

Es innegable el impacto que ha tenido la entrada en vigor en 2018 del Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) en la actualización de las legislaciones de protección de datos en todo el mundo, en la región y, por ende, sobre Argentina. El RGPD sienta condiciones para quienes, en un entorno globalizado con crecientes flujos transfronterizos de datos, quieran dinamizar su economía a través del intercambio de bienes y servicios con las garantías adecuadas para la protección de los datos personales de su ciudadanía.

La referencia al RGPD es importante en este contexto dado que Argentina, al sumarse al Convenio 108+ en septiembre de 2019 y su reciente ratificación, asume el compromiso de mantener su marco regulatorio interno conforme a los estándares internacionales actuales, en gran medida demarcados por la nueva normativa europea. La vigente Ley 25.326, sancionada en octubre del año 2000, pese a ser una regulación pionera en su momento, hoy resulta insuficiente dado el gran avance de la tecnología, el masivo procesamiento de datos y las exigencias regulatorias dispuestas en otras regiones para el intercambio de datos.

En el proceso de elaboración de la reforma de esta normativa es menester comprender la

evolución del derecho a la protección de los datos personales. Este derecho actualmente es transversal puesto que va más allá de la privacidad y se constituye como una garantía para el libre ejercicio de otros derechos como el de autodeterminación informativa, libertad de expresión, participación ciudadana, entre otros. Su objetivo será el de establecer reglas para el desarrollo de actividades que involucren la recolección y procesamiento de datos. Así como también, prevenir injerencias arbitrarias en el normal desenvolvimiento de la vida de los ciudadanos, a diferencia de otras regulaciones que buscan de forma reactiva brindar mecanismos de reparación frente a vulneraciones, como sucede con el ya existente habeas data.

A continuación, nos referimos a los aspectos que consideramos indispensables para una reforma de ley integral de protección de datos personales, que sentimos requieren de un oportuno énfasis y que refuerzan la necesidad de adaptar el actual marco regulatorio.

1. Proceso multiparticipativo

Dada la complejidad de la materia y su relevancia en la sociedad actual, es fundamental que el proceso de elaboración del proyecto de reforma garantice que la discusión se lleve a cabo de manera abierta, transparente, e inclusiva. Esto implica llevar a cabo consultas públicas y mesas redondas abiertas de personas expertas, publicar los textos de negociación y permitir comentarios de las partes interesadas con fechas límite razonables, y brindar una retroalimentación sobre los comentarios recibidos. En todas las etapas, debe asegurarse la participación significativa de los grupos de la sociedad civil, y todas las reuniones con la industria, las ONG, y los grupos de consumidores deben hacerse por medio de un llamado público ampliamente difundido. El objetivo principal debe ser asegurar la igualdad entre los distintos sectores para compensar el desequilibrio inevitable con respecto al número de voces en comparación con la industria.

2. Lista de principios que rigen el tratamiento de datos

A continuación listamos algunos de los principios vinculantes de común inclusión a nivel internacional que permite orientar el régimen de protección de datos personales:

a. Legalidad: todo tratamiento de datos debe tener una base jurídica clara, con un propósito claro, y de una manera justa y transparente.
b. Limitación de la finalidad: el propósito de la recolección y procesamiento debe ser específico, explícito, y de duración limitada.
c. Minimización de dato: los datos personales recopilados y utilizados deben limitarse a ser suficientes, pertinentes y no excesivos en relación con un propósito específico y definido.
d. Exactitud y calidad: los datos personales deben ser precisos y, cuando corresponda, deben ser actualizados. Las personas titulares deben tener el derecho a eliminar, rectificar, y corregir su información personal.
e. Conservación limitada: los datos personales procesados por cualquier propósito no deben ser mantenidos por más tiempo del necesario.
f. Seguridad de los datos: los datos personales deben ser procesados de manera que se garantice una seguridad de vanguardia para los datos, junto con la

protección contra tratamiento no autorizado o ilegítimo y contra la pérdida accidental, destrucción o daños de los datos, utilizando medidas técnicas y organizacionales pertinentes.

g. Confidencialidad: el responsable de datos personales y quienes tengan acceso a ellos deberán guardar secreto o confidencialidad acerca de los mismos. El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.
h. Transparencia e información: las políticas y las prácticas sobre el tratamiento de los datos personales deben estar permanentemente accesibles y a disposición de cualquier interesado de manera precisa, clara, inequívoca y gratuita.
i. Responsabilidad: quienes realicen tratamiento de los datos personales serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad a la ley.

3. Independencia y sustento de la autoridad de aplicación

Por más valioso y ajustado a los estándares internacionales que sea el contenido de la propuesta legislativa, su aplicación puede verse seriamente afectada en caso de no establecer y garantizar la absoluta independencia de la autoridad de aplicación tanto del sector privado como del sector público. Tal es así, que los marcos regulatorios más modernos encuentran en este aspecto el mayor desafío, vaciando de contenido aquello que se logró plasmar en el cuerpo legal. Por ello, tanto la designación como la remoción de quien o quienes integren su dirección debe realizarse con acuerdo del Senado y en base a una lista de candidatos previo concurso de competencia dada la complejidad de la materia.

Para su efectivo funcionamiento es necesario además dotarla de recursos humanos y materiales suficientes. Las obligaciones encomendadas a la autoridad son extensas por lo que su presupuesto debe estar a la altura de la función que debe desempeñar.

4. Multas disuasorias

Una de las razones fundamentales que motivaron la actualización de la normativa europea fue la necesidad de aumentar los montos de las multas que justifique a las empresas cumplir con la ley. Es que para los grandes procesadores de datos que surgieron en las últimas décadas era más beneficioso violar la ley y pagar las sanciones que ajustar su estructura para estar en norma.

Este mismo problema tiene nuestra ley actual, agravado por el contexto económico actual. Por ello, una reforma de ley debe establecer para el sector privado multas conformadas en base a un porcentaje de los ingresos del periodo anterior de las empresas. Esto permite la progresividad de la multa, es decir, permite tener en cuenta la envergadura de la organización tratadora de datos.

En el caso de particulares, organizaciones sin fines de lucro y del sector público, más allá de las medidas correctivas y los apercibimientos disciplinarios que dispongan otras normas, debe establecerse una sanción al responsable determinada en base a unidades fijas (como el Salario Mínimo Vital y Móvil).

5. Limitación a las excepciones al consentimiento como fuente de legitimidad

La moderna doctrina en protección de datos personales coincide en establecer al consentimiento como la regla general para el tratamiento de datos. Si bien existen legítimas excepciones, es fundamental evitar que estas den lugar a abusos y creen lagunas o vacíos legales que eviten su efectiva aplicación. Tanto la seguridad pública como el interés legítimo de las empresas han sido abusados en normativas comparadas y en regulaciones de otras materias.

Es exactamente esto lo que ha sucedido con lo dispuesto por el artículo 5 inciso 2.b. de la ley 25.326 que permite el tratamiento de datos personales sin consentimiento de las personas titulares cuando "*Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal*". Disposiciones como esta deben ser eliminadas por ser contrarias al espíritu de las leyes de protección de datos personales, a sus principios e impiden el ejercicio de los derechos.

6. Procedimiento y obligatoriedad de vulneraciones de seguridad

La actual ley carece de un proceso por el cual los responsables del tratamiento se vean obligados a notificar violaciones de la seguridad de los datos personales a la autoridad de aplicación y a las personas titulares de los datos.

Dicho procedimiento debe ajustarse a los estándares en materia de seguridad de la información, estableciendo un plazo no superior a 72hs desde el anoticiamiento de la vulneración, el registro de los acontecimientos, canales seguros de denuncia, y los escenarios en los que debe comunicarse con la mayor anticipación posible a las personas titulares para que adopten medidas de seguridad adicionales. Tal es la relevancia de esta obligación que su incumplimiento debe estipularse como una falta grave.

7. Encargado de protección de datos personales

Las modernas normativas regionales e internacionales incorporan la creación del "encargado de protección de datos personales" como aquella persona física o jurídica, interna o externa a la organización, que tiene como función colaborar en el cumplimiento de la ley, mejorar las políticas internas de las organizaciones e instituciones, recibir denuncias y dar lugar al ejercicio de derechos entre otras atribuciones.

Los estándares de la Red Iberoamericana de Protección de Datos (RIPD)[1], por ejemplo, establecen que debe ser obligatoria la designación de un encargado en el caso de autoridades públicas, cuando se lleve a cabo el tratamiento de datos personales que tenga por objeto una observación habitual y sistemática de la conducta del titular, cuando se realice tratamiento de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales, y en aquellos casos que lo amerite teniendo en cuenta factores como la categoría de datos personales tratados (en especial, datos sensibles), las transferencias que se utilicen, el número de las personas titulares, el alcance del tratamiento, las tecnologías de información utilizada o la finalidad del tratamiento.

8. Categorías especiales de datos personales

Si bien la actual ley de protección de datos personales incluye a los datos sensibles, la reforma de ley debe crear una sección que contenga categorías especiales de datos personales que defina a los datos sensibles de manera no taxativa y mencionar los datos genéticos y biométricos, diagnósticos de salud mental o física, historial sobre sexualidad o vida sexual, historial sobre delitos civiles o penales, afiliación política, afiliación religiosa, como cualquier otro dato o dato inferido que pueda implicar una discriminación arbitraria.

Al mismo tiempo, debe cambiar su lenguaje de “nadie está obligado a brindar datos sensibles” por la prohibición general del tratamiento de estas categorías especiales autorizando solo si las personas titulares expresan libremente su consentimiento explícito e informado o si la ley lo autoriza explícitamente en forma proporcional y necesaria a la finalidad legítima perseguida. En ambos casos se deben establecer resguardos respecto de quién tiene acceso, quién puede utilizar esta información y con qué finalidad. Debe incluir el derecho a rehusarse a que se almacenen los datos personales sensibles.

Las categorías especiales deben incluir los datos relativos a niños, niñas y adolescentes. Por las mismas razones expuesta a los datos sensibles, su tratamiento debe estar condicionado al cumplimiento de requisitos restrictivos y que tengan como objetivo la protección de esta categoría de titulares. En este sentido, no corresponde que los datos de niñas, niños y adolescentes puedan ser tratados libremente ni aún por tratarse de datos de naturaleza pública.

La normativa debe incluir explícitamente medidas especiales para la protección de los datos de tráfico de las comunicaciones o metadatos y de los datos personales registrados a partir de actividades de internet de los y las usuarias, debido a que esta información revela rasgos personales particularmente sensibles. Los metadatos contenidos en las comunicaciones telefónicas, en el correo electrónico, en las fotografías digitales o en los registros de acceso a redes sociales permiten identificar a la persona, localizarla geográficamente y revelar las características de los dispositivos que usa, lo que la hace más vulnerable a la vigilancia por parte del Estado o de otros privados. La Ley de Protección de Datos Personales debe incluir

[1] https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

disposiciones para regular la captura, almacenamiento y tratamiento de datos que obtienen los dispositivos inteligentes, así como la obligación de proporcionar información clara a las personas titulares para que tomen decisiones sobre el uso de estos aparatos.

9. Protección de datos personales por diseño y por defecto

Esta nueva figura, incorporada mayoritariamente por el derecho comparado, tiene por finalidad exigir y garantizar que la privacidad y la protección de datos sean tomadas en cuenta por los ingenieros en la fase de diseño de productos y servicios, y que estén configurados en el nivel de protección más alto por defecto. Al incluirla, las compañías toman una postura positiva para proteger los derechos de las personas titulares de los datos, ya que se incorporan principios que protegen la privacidad tanto en las políticas tecnológicas como en las organizacionales. La privacidad y la protección de datos se vuelven parte de la cultura y el marco de la rendición de cuentas de la compañía, en lugar de ser un “simple elemento de cumplimiento”. Permite, a su vez, simplificar costos, realizar ajustes para el cumplimiento de la ley y reducir los riesgos de vulneraciones de seguridad.

10. Estudios de impacto sobre la protección de datos personales

La reforma de la ley debe incluir la exigencia de elaborar estudios de impacto sobre la protección de los datos personales previo a la oferta o implementación de una tecnología y de forma periódica cuando lo amerite. Debe estipular el procedimiento, los elementos que debe contener y los casos en los que debe ser obligatorio. Respecto a este último elemento nos remitimos a los casos sugeridos en el punto 7 respecto al encargado de datos personales.

A su vez, debe permitirle a la autoridad de aplicación por medio de reglamento, extender la listas de casos obligatorios, los requisitos y cualquier otro elemento que sea necesario en base a la evolución de las actividades de procesamiento de datos.

11. Mecanismos vinculantes, seguros y transparentes para la transferencia segura de datos a terceros países

La reforma de la ley debe estar diseñada para garantizar la libre circulación de datos, estableciendo mecanismos para la transferencia de datos y salvaguardas para los derechos de las personas titulares. Estos mecanismos deben estar sometidos a una supervisión estricta y transparente, e incluir medidas de reparación para garantizar que los derechos de las personas titulares viajen junto con los datos.

Por ello, entre otras de las disposiciones que deben incluirse para cumplir con este requisito, el proyecto debe estipular un claro ámbito de aplicación territorial que permita aplicar la ley no solo a aquellas empresas, particulares e instituciones que se encuentren en el país sino también a las que se encuentran fuera del territorio nacional y que procesan datos de la ciudadanía argentina. Además, debe incluir mecanismos por los cuales se establezca que un determinado país garantiza una adecuada protección de los datos personales.

Estas medidas jurisdiccionales pueden evitar una espiral descendente en términos de protección, por la cual ciertas industrias decidirían reubicar sus compañías fuera de un país para evitar la aplicación de medidas que protejan al usuario.

12. Derecho a no ser sometido a decisiones automatizadas o parcialmente automatizadas

El desarrollo de tecnologías de inteligencia artificial ha dado como resultado la necesidad de crear este nuevo derecho que tiene por objetivo proteger a las personas de las tomas de decisiones arbitrarias que estas tecnologías suelen adoptar producto de sus parcialidades intrínsecas.

El derecho permite a las personas titulares de los datos negarse a dichos procedimientos en especial cuando tienen por finalidad la elaboración de perfiles. El agregado “parcialmente automatizadas” es necesario por cuanto muchas empresas incluían a una persona al final de la cadena de la toma de decisión con injerencia nula para evitar que se haga uso de este derecho. Incluso, se le debe permitir a las personas titulares que soliciten la intervención significativa de un humano.

Petitorio

Solicitamos la apertura de un proceso inclusivo, público y abierto para todas las etapas de elaboración y discusión de un proyecto de reforma, y se tenga en cuenta estos aportes con la finalidad de que la normativa de protección de datos que se apruebe en definitiva refleje los elementos esenciales para asegurar a las personas titulares control sobre sus datos y garantizar el ejercicio de los derechos de toda la ciudadanía argentina.

Firmantes

Access Now
Asociación por los Derechos Civiles (ADC)
Centro de Estudios en Tecnología y Sociedad (CETyS)
Data Governance Latam
Datas | Tech Governance
Democracia en Red
Fundación Vía Libre
Observatorio de Derecho Informático Argentino (O.D.I.A.)