

Proyecto de Ley de (Des)Protección de Datos Personales

¿Un avance o una oportunidad perdida?

Resumen Ejecutivo

El proyecto de protección de datos personales propuesto por el Poder Ejecutivo tiene la apropiada vocación de modernizar la regulación en Argentina a la luz de diversos avances, en particular, en materia de negocios de la economía digital. Sin embargo, tiene algunos aspectos problemáticos que la tornan inviable para el logro del objetivo mentado de proteger los derechos de la ciudadanía.

Entre los problemas más destacados del proyecto podemos mencionar:

- La no incorporación de los datos biométricos y genéticos como datos sensibles, lo que deja este tipo de datos a merced de la protección más laxa de la norma.
- La inclusión de la figura del consentimiento tácito.
- La habilitación a las empresas de trasladar libremente los datos personales a través de las fronteras.
- Las nulas protecciones de los ciudadanos frente al Estado.
- El mantenimiento de una autoridad de aplicación y control subsumida al Poder Ejecutivo.

Estas y otras razones tornan problemática la aprobación de esta ley tal como fue enviada por el PEN al Senado y hace indispensable la apertura y ampliación del debate parlamentario para la construcción de una regulación garante del principio constitucional de Habeas Data y del derecho a la intimidad de las personas en Argentina.

Introducción

El 19 de Septiembre pasado, el Poder Ejecutivo Nacional envió al Senado de la Nación el [Mensaje 147-2018](#) tendiente a reemplazar la actual ley de Protección de Datos Personales. El proyecto tiene como principal aspiración la actualización de las normas de protección de datos en Argentina, en particular, tras la entrada en vigencia del Reglamento Europeo de Protección de Datos en mayo de este año.

Sin embargo, y pese a la notable inspiración que tiene el proyecto en el RGPD de la UE, en líneas generales establece una serie de flexibilidades y excepciones que desprotegen a los ciudadanos frente al Estado y frente al sector privado, especialmente, frente al sector de la economía de la información que tiene en los datos personales el insumo fundamental de su negocio.

Para entender las ventajas y las flaquezas del proyecto es fundamental analizar parte por parte y destacar además las actualizaciones que propone en una materia fundamental para los derechos en el siglo XXI.

El objeto de la ley

La ley tiene por objeto derogar y reemplazar la ley de protección de datos vigente y establecer un nuevo régimen de protección de los datos personales en Argentina. En este sentido, inicia el texto con la definición de datos personales y datos sensibles.

Dos definiciones fundamentales para comprender el proyecto:

Datos personales: información de cualquier tipo referida a personas humanas determinadas o determinables, inclusive los datos biométricos. Se entenderá por determinable la persona que pueda ser identificada mediante algún identificador o por uno o varios elementos característicos de la identidad física, fisiológica, genética (datos genéticos), psíquica, económica, cultural o social de dicha persona. No será considerada persona determinable cuando, para lograr su identificación, se requiera la aplicación de medidas o plazos desproporcionados o inviables. Se entenderá por datos biométricos aquellos datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única. Se entenderá por datos genéticos los relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud, obtenidos en particular del análisis de una muestra biológica.

Datos sensibles: datos personales que afectan la esfera íntima de su titular con potencialidad de originar una discriminación ilícita o arbitraria, en particular, los que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, participación o afiliación en una organización sindical o política, información referente a la salud, preferencia o vida sexual.

Encontramos aquí una primera divergencia seria con el Reglamento de la Unión Europea. El proyecto de ley argentino **no considera como datos sensibles los datos biométricos y los datos genéticos de la ciudadanía**. En el reglamento europeo, ambas categorías de datos gozan de las más altas protecciones y son considerados datos sensibles ([Véase artículo 9 del RGPD de la UE](#)).

En el trámite parlamentario, los datos genéticos y los datos biométricos deberían ser incorporados y protegidos bajo la misma categoría que los datos sensibles.

Ámbito de aplicación de la norma

Al igual que en el caso del RGPD de la UE, el ámbito de aplicación está enfocado en el titular de los datos. Entonces, las obligaciones dimanantes del proyecto alcanzan a todo aquel que realiza tratamiento de datos de personas que residen en el territorio de la República Argentina.

Principios relativos al tratamiento de los datos

El principio de **finalidad** de los datos es uno de los resguardos más importantes de la doctrina de protección de datos. Significa, en líneas generales, que un dato no puede ser usado para una finalidad diferente a la que dio origen a su recolección. En este sentido, el principio de finalidad debe ir de la mano del consentimiento informado a la hora de otorgar permisos de uso de los mismos. El proyecto establece que “los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no deben ser tratados de manera incompatible con dichos fines.”

Hasta aquí, el proyecto reproduce la doctrina del Reglamento Europeo (Cap. II Art. 5, inciso b) que no considera incompatibles los tratamientos ulteriores de los datos con fines de archivo de interés público, investigación científica e histórica o fines estadísticos.

Sin embargo, agrega una cláusula inadmisibles, al abrir el juego a cualquier otros usos que pudieran ser, “*de acuerdo al contexto, razonablemente presumidos por el titular de los datos*”-.

El principio de finalidad se torna así una mera declaración, ya que no hay definición alguna ni límite que permita suponer a qué se denomina un fin “*razonablemente presumido*” según el contexto. Es recomendable eliminar esta fórmula que borra con el codo la definición del principio de finalidad de los datos.

El principio de minimización implica que los datos deben ser tratados de manera adecuada, pertinente y limitados a lo necesario en relación a los fines para los cuales fueron recolectados. Por lo tanto, si el fin del dato no es claro o es difuso y laxo, el principio de minimización también puede convertirse en letra muerta.

Lo mismo ocurre con los plazos de conservación, que están limitados al tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

El artículo sobre **Consentimiento** merece un párrafo aparte, ya que es uno de los que genera mayores dudas y problemas. Se trata del **Artículo 12** del proyecto que 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.

La forma del consentimiento depende de las circunstancias, el tipo de dato personal y las expectativas razonables del titular de los datos. Así, el consentimiento expreso puede ser obtenido de acuerdo a circunstancias particulares, de forma escrita, verbal, por medios electrónicos o cualquier otra forma similar que la tecnología habilite. Sin embargo, presenta aquí la figura del consentimiento tácito, admitido cuando surja de manera manifiesta del contexto del tratamiento de los datos y la conducta del titular sea suficiente para demostrar la existencia de su autorización.

Este aspecto es una verdadera caja de sorpresas y debería ser excluido del texto de la ley en el trámite parlamentario, ya que desprotege completamente a los titulares de derechos. ¿Qué se entiende por consentimiento tácito? ¿El mero uso de una aplicación podría ser considerado una forma de consentimiento para que los responsables del tratamiento de los datos consideren que hubo consentimiento tácito? La vaguedad y riesgos implícitos en este apartado tornan indispensable una discusión más profunda.

Al menos, vale destacar que los datos sensibles sólo pueden ser tratados bajo consentimiento expreso. Sin embargo, recordemos que los datos genéticos y los datos biométricos no tienen calidad de datos sensibles en este proyecto de ley, por lo que podrían ser pasibles de trámite con el simple consentimiento tácito.

El consentimiento debe poder ser revocado de forma sencilla, gratuita y por la misma vía que se obtuvo el consentimiento. Sin embargo, nada aclara el proyecto de ley sobre cómo se revoca el consentimiento tácito. Por cierto, la revocatoria no tiene efectos retroactivos.

Un artículo para eliminar el fallo Torres Abad

El artículo 14 del proyecto merece ser destacado. Expresa literalmente:

ARTÍCULO 14.- Excepciones al consentimiento previo. No es necesario el consentimiento para el tratamiento de datos cuando se trate de listados cuyos datos se limiten a nombre y apellido, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y correo electrónico, ni para el tratamiento de la información crediticia en los términos del Capítulo 6.

En el [Fallo Torres Abad c/ Jefatura de Gabinete de Ministros](#), la Cámara fija límites claros y establece que si la titular de los datos no presta consentimiento expreso para el tratamiento de los mismos, el organismo que los obtuvo, en este caso ANSES, no puede cederlos ni darlos a conocer, ya que se encuentran protegidos bajo la ley 25.326 de Protección de datos personales.

Esa protección que claramente está en la ley actual se borra completamente en caso de que el artículo 14 de este proyecto sea aprobado. Es, claramente, un artículo destinado a revertir este fallo contrario a la posición de la Jefatura de Gabinete de Ministros, organismo que presentó el proyecto de Ley y del que además depende la autoridad de aplicación de protección de datos.

Transferencia internacional de los datos

La transferencia internacional de los datos personales es uno de los temas más sensibles de las últimas décadas en lo que a derecho a la privacidad se refiere. Es el tema central de la agenda de comercio electrónico de la Organización Mundial de Comercio sobre el cual trabajamos con diversas organizaciones en el marco de la Reunión Ministerial en Buenos Aires.

Este tema clave se encuentra reflejado en el proyecto, específicamente en el artículo 23 que establece las pautas para la transferencia internacional y las flexibiliza de una forma preocupante.

Especialmente problemático es el inciso e) que otorga a las empresas la potestad de mover los datos a través de las fronteras libremente:

Toda transferencia internacional de datos personales es lícita si se cumple al menos UNA (1) de las siguientes condiciones:

- a. Cuento con el consentimiento expreso del titular de los datos;
- b. El país u organismo internacional o supranacional receptor proporcione un nivel de protección adecuado;
- c. Se encuentre prevista en una ley o tratado en los que la REPÚBLICA ARGENTINA sea parte;
- d. Sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
- e. Sea efectuada a cualquier sociedad del mismo grupo económico del responsable del tratamiento, en tanto los datos personales sean utilizados para finalidades que no sean incompatibles con las que originaron su recolección;
- ...
- l. Tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el lavado de activos, los delitos informáticos y el narcotráfico;

De esta forma, queda habilitada una de las demandas del grupo GAFAA (Google, Amazon, Facebook, Apple y Ali Baba) ante los foros internacionales. Es destacable otra característica especificada aquí: la habilitación prevista en una ley o tratado en los que la República Argentina sea parte (podría incluirse una cláusula de este tipo en tratados comerciales en negociación). El apartado incluye además cualquier acuerdo de intercambio de datos de inteligencia que Argentina tenga rubricado con otros países, información que las organizaciones integrantes de la Iniciativa Ciudadana de Control de los Organismos de Inteligencia solicitamos mediante una nota de Acceso a



Fundación
Vía Libre

la Información a la AFI. Por supuesto, esa información no fue suministrada bajo el amparo de las normas de Secreto.

Derechos de los titulares de los datos

Los titulares de los datos tienen plenos derechos sobre los mismos, tal como ya está consagrado en la doctrina de protección de datos local. En este nuevo proyecto, el artículo 28 establece una serie de especificaciones sobre los derechos de los titulares al expresar:

ARTÍCULO 28. - Contenido de la información. La información debe ser suministrada en forma clara, exenta de codificaciones y, en su caso, acompañada de una explicación de los términos que se utilicen, en lenguaje accesible al conocimiento medio de la población, y debe versar sobre:

- a. Las finalidades del tratamiento de datos;
- b. Las categorías de datos personales de que se trate;
- c. Los destinatarios o las categorías de destinatarios a los que se cedieron o se prevean ceder los datos personales, en particular cuando se trate de una transferencia internacional;
- d. El plazo previsto de conservación de los datos personales o, de no ser ello posible, los criterios utilizados para determinar este plazo;
- e. La existencia del derecho a solicitar del responsable del tratamiento la rectificación, supresión de datos personales o a oponerse a dicho tratamiento;
- f. El derecho a iniciar un trámite de protección de datos personales ante la autoridad de control;
- g. Cuando los datos personales no se hayan obtenido del titular de los datos, cualquier información disponible sobre su origen;
- h. La existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 32 y, al menos en tales casos, información significativa sobre la lógica aplicada, sin que ello afecte derechos intelectuales del responsable del tratamiento.

Este inciso h) es clave y forma parte de la actualización de este proyecto de ley, ya que trata justamente de las regulaciones realizadas mediante el uso de algoritmos, uno de los temas centrales de la economía de la Big Data. En este sentido, el proyecto adopta la terminología del Reglamento Europeo, sin embargo, a diferencia de aquel, no consagra el derecho a que esas decisiones automatizadas sean revisadas por un humano. Este resguardo debería ser incorporado en el trámite

parlamentario. Además, entre el derecho del titular de los datos a la información sobre ese procesamiento y la propiedad intelectual de la empresa u organismo responsable del tratamiento, prioriza la protección de los derechos intelectuales de este último.

Sobre el tratamiento automatizado, el proyecto agrega:

ARTÍCULO 32.- 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.

El titular de los datos no podrá ejercer este derecho si la decisión:

- a. Es necesaria para la celebración o la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento;
- b. Está autorizada por Ley;
- c. Se basa en su consentimiento expreso.

En los casos a que se refieren los incisos a) y c), el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos del titular de los datos.

Responsabilidades del responsable del tratamiento de los datos

La norma incorpora algunos aspectos importantes tendientes a mejorar el cumplimiento de la normativa por parte del sector privado. Entre ellas, la realización y presentación ante la autoridad competente de **evaluación de impacto** que puede generar el tratamiento de datos personales, así como la designación de un **Delegado de Protección de datos Personales** cuando:

- a. Cuando revistan el carácter de autoridades u organismos públicos;
- b. Se realice tratamiento de datos sensibles como parte de la actividad principal del responsable o encargado del tratamiento;
- c. Se realice tratamiento de datos a gran escala.

Supuestos especiales

El marco normativo propuesto incluye el tratamiento de los datos personales que realicen las fuerzas de seguridad y los organismos de inteligencia. De esta forma, el proyecto de ley establece:



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.

Se deben suprimir, aun si no mediare solicitud del titular, los datos personales de las bases de datos mencionadas en el párrafo anterior cuando no sean necesarios para los fines policiales que motivaron su recolección.

Un tema aparte merece el artículo 68, que literalmente habilita el **Spam**.

ARTÍCULO 68.- Bases destinadas a la publicidad. 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 previstos en la presente Ley.

La autoridad de aplicación y control del cumplimiento de la ley

La normativa vigente de protección de datos tiene una flaqueza central, fruto del veto presidencial del entonces Primer Mandatario Fernando De La Rúa en 2001. Se trata de la figura de la Autoridad de Aplicación.

El proyecto de ley no repara esa flaqueza y establece que la Autoridad de Protección de Datos personales seguirá siendo la actual oficina en el marco de la Oficina de Acceso a la Información Pública dependiente de la Jefatura de Gabinete de Ministros. Es decir, una autoridad de aplicación incapaz desde el propio diseño institucional, de ejercer pleno control contra los potenciales abusos que puedan cometer organismos públicos (para muestra, vale mencionar el dictamen favorable de la Dirección Nacional de Protección de Datos Personales al traspaso de la base de datos de ANSES a Jefatura de Gabinete de Ministros en 2016).



En el caso de las consecuencias que tendrá no cumplir con la ley, hay una diversidad de acciones que van desde el apercibimiento hasta una multa de hasta 500 salarios mínimo, vital y móvil, incluyendo el cierre temporal de la operación que involucre el tratamiento de datos y el cierre definitivo de las operaciones que involucren el tratamiento de datos sensibles.

Sin embargo, el incumplimiento de la ley por parte de un organismo público sólo generará la apertura de un expediente interno de investigación por parte del mismo organismo que incumple la norma. Esto deriva en más desprotección para los ciudadanos frente a los potenciales abusos por parte del Estado y/o los funcionarios públicos.

Consideraciones finales

En resumen, la iniciativa del Poder Ejecutivo Nacional puesta a consideración del Congreso pretende modernizar la terminología y el alcance de la protección de datos vigente en Argentina, pero de aprobarse tal como fue propuesta, será una oportunidad perdida en ese sentido.

En líneas generales, otorga potestades demasiado amplias para el tratamiento de datos por parte del sector privado, incluyendo aspectos directamente inaceptables como el consentimiento tácito o el prácticamente libre tráfico transfronterizo de datos personales. La virtual legitimación del Spam parece incluso una burla mientras que la inclusión del registro No Llame constituye una medida más afín con la defensa del consumidor que con la protección de datos personales.

La exclusión de los datos genéticos y los datos biométricos de la definición de datos sensibles supone una desprotección absoluta de estos datos que contienen una carga de información fundamental sobre las personas. Libera de este modo la posibilidad de establecer bases de datos que contengan esa información sin los controles apropiados propios de la información sensible. Esta cláusula es claramente contraria a la doctrina vigente en el Reglamento Europeo.

También es grave la potestad casi total que le otorga a las oficinas estatales para la gestión de los datos que los ciudadanos deben entregar para el cumplimiento de sus funciones, la prácticamente nula sanción en caso de incumplimiento de la normativa y la habilitación casi irrestricta para el libre uso de datos por parte de los funcionarios de la administración pública.



Argentina tiene ante este proyecto la posibilidad de mejorar la legislación vigente con la creación de una autoridad de aplicación autónoma, autárquica, con potestades plenas para velar por los derechos de los ciudadanos. La propuesta no recoge nada de esto. Sin una autoridad de aplicación adecuada, cualquier ley, independientemente de su calidad, puede terminar en letra muerta. El Congreso debería insistir con la creación de un órgano de control apropiado a los desafíos de nuestro tiempo.

El debate global sobre la protección de datos personales está abierto. Argentina tiene ahora la oportunidad de establecer una regulación que garantice el pleno ejercicio de los derechos fundamentales de la ciudadanía. Si el proyecto avanza tal como fue previsto por el PEN seremos testigos, una vez más, de una oportunidad perdida.