
# Propuesta de Anteproyecto de Ley de Protección de Datos Personales. Agencia de Acceso a la Información Pública. Septiembre 2022.

**Por Flor Azategui Zabala.**

**Sumario: I. ¿ DE QUÉ SE TRATA?. II. LO NOVEDOSO. III. LO "MEJORABLE".**

## I. ¿ DE QUÉ SE TRATA?.

Durante el mes de Septiembre, la **Agencia de Acceso a la Información Pública** (AAIP) -dependiente de la Jefatura de Gabinete de Ministros-, actualmente a cargo de la Mg. Beatriz Anchorena, elaboró una **Propuesta de Anteproyecto de modificación de la Ley 25.326, de Protección de Datos Personales** (LPDP)[1].

La 25.326, recordemos, fue sancionada en el año 2000 y con más 20 años de antigüedad, en un contexto tecnológico que cambia y evoluciona de manera exponencial, ha quedado obsoleta. En este contexto es que interviene la AAIP elaborando dicho Anteproyecto.

Ante todo, es importante destacar que el Anteproyecto sigue los lineamientos de las últimas legislaciones en materia de protección de datos personales aprobadas en el mundo, como el Reglamento General de Protección de Datos de la Unión Europea (RGPD), la Ley General de Protección de Datos de Brasil o la Ley Orgánica de Protección de Datos de Ecuador, entre otras.

El **objeto** de la LPDP es *asegurar la protección de los datos personales de las y los individuos, reglamentar el debido tratamiento de dichos datos y delimitar los deberes de quienes intervengan en tales tratamientos de datos personales*.

## II. LO DESTACABLE.

DISPOSICIONES GENERALES.

En las Disposiciones Generales agrega deberes para quienes realizan el tratamiento. Agrega definiciones como "Datos Biométricos", "Genéticos", "Delegado de Protección de Datos Personales" (DPDP), "Elaboración de Perfiles", "Grupos Económicos", "Incidentes de Seguridad", "Responsable de Datos", "Encargado de Datos", "Seudonimización".

Protege al Dato Personal aún cuando no forme parte de una base de datos.

Incluye como sujetos obligados a las Fuerzas Armadas, de Seguridad e Inteligencia.

TRATAMIENTO DE DATOS.

En cuanto al tratamiento de datos, establece que la **recolección** debe ser **lícita, leal** y **transparente**.

Su **finalidad** debe ser **determinada, explícita y legítima.** Y puede ser realizada con fines estadísticos y/o de archivo.

Establece el **Principio de Minimización de Datos**, que implica que los datos recolectados deben ser solo los necesarios para su finalidad.

El Anteproyecto plantea que las entidades -privadas y públicas- que traten datos deberán obrar con **responsabilidad proactiva** y **demostrada**.

[1] La AAIP es la **autoridad de aplicación** de la LPDP y del Registro Nacional No Llame. Además, tiene el deber de recibir y gestionar las solicitudes de información pública, principalmente efectuadas por la ciudadanía.

En el sector público, establece la **responsabilidad compartida** para el caso de cesiones de datos. Para ello, instituye las figuras de Responsables, Encargados, Representantes, Terceros y Delegados en el tratamiento de los datos.

También, privilegia los derechos de los datos personales de las infancias conforme a diversos instrumentos internacionales.

Además, se refuerzan las características que debe tener el **consentimiento:** el Titular del dato debe prestar su consentimiento para el tratamiento de manera *libre, específica, informada e inequívoca*, mediante una *declaración* o *clara acción afirmativa*. La **revocación** de tal consentimiento debe ser *fácil, gratuita, expedita*.

Busca ampliar la definición de **datos sensibles**[2], incorporando dentro de este concepto a los datos **genéticos** y **biométricos**. Y, establece mayor nivel de responsabilidad, confidencialidad, seguridad, restricciones de uso y circulación de dicha categoría de datos. Prohíbe a los prestadores de salud del sector privado utilizar datos para selección de riesgo o exclusión de beneficiarios.

EXTRATERRITORIALIDAD.

El Anteproyecto, busca ampliar el ámbito de aplicación de la Ley, ya que exige el respeto de los derechos de las/los ciudadanas/os argentinas/os frente a entidades extranjeras que -aunque no tengan domicilio legal en el país- recolectan datos personales. Es decir, incorpora el concepto de **extraterritorialidad**, para los casos en que los responsables del tratamiento no se encuentren en el país.

DERECHOS SOBRE LOS DATOS.

En cuanto a los derechos de los Titulares de datos, se incluyen los de **acceso, oposición, portabilidad, rectificación, supresión y control sobre las inferencias**[3] (es decir, sobre los datos inferidos de la persona). Así, cada titular tiene derecho a que se le informe sobre la finalidad del tratamiento, el tiempo del mismo, si el tratamiento es automatizado, cómo se realiza, etc. Dicha información debe ser suministrada de forma **clara, completa, veraz y exenta de codificaciones**.

Establece que no puede haber resultados basados en decisiones tomadas mediante sistemas de tratamiento automatizado o semiautomatizado de datos, cuyos parámetros sean aspectos étnicos, raciales, filosóficos, religiosos, políticos, morales sindicales, de orientación sexual, etc. Incluso, otorga el derecho a obtener intervención humana del Responsable y requerir la exhibición de los patrones de programación del algoritmo cuando intervengan en el tratamiento dichos sistemas.

INCIDENTES DE SEGURIDAD.

Sobre los **incidentes de seguridad,** especifica que **son atentados contra la confidencialidad, integridad y disponibilidad de los datos**. Establece, para el Responsable, la obligación de notificación a la Autoridad de Aplicación y a los Titulares de los datos, dentro del plazo de 48 horas de haber tomado conocimiento y de forma **clara, expedita y sencilla**.

INFORMACIÓN CREDITICIA Y DERECHO AL OLVIDO.

El Anteproyecto incluye artículos referidos a **datos de información crediticia**, estableciendo que podrán ser conservados por hasta 5 años -o 1 año cuando se cancele o extinga la obligación- y que, de ser requerido por el titular, las entidades deberán comunicar detalladamente cuál es la fórmula o al algoritmo utilizado. Las compañías también *"deben comunicar al titular de los datos cuando cambie su situación crediticia"*.

AUTORIDAD DE APLICACIÓN. FACULTADES Y SANCIONES.

Se establece que la Autoridad de Aplicación puede solicitar autorización judicial para el auxilio de la fuerza pública, con la finalidad de hacer cumplir la ley.

---

[2] Datos Sensibles son aquellos que se refieren a la esfera íntima de las personas, o pueden generar discriminación o riesgo grave para el/la titular.

[3] Una inferencia se produce cuando se realiza análisis de datos y se infiere algo en función de ellos, como la pertenencia a determinados grupos por ciertas compras o likes, por ejemplo.

También, puede -y debe- emitir la normativa reglamentaria necesaria, tramitar denuncias interpuestas por interesados, solicitar información a Encargados o Responsables, implementar mecanismos voluntarios de solución de controversias, constituirse en querellante en acciones penales, promover acciones de cooperación con entidades extranjeras, asistir y asesorar a organismo públicos respecto del cumplimiento de la ley, investigar, desarrollar conocimiento, divulgar información sobre los extremos de esta ley, entre otras atribuciones.

En lo referido a las **sanciones**, establece que los procedimientos administrativos o judiciales pueden ser iniciados por el Titular del dato, la Autoridad de Aplicación o un tercero interesado; a través de cualquier medio habilitado a tales efectos y de manera gratuita.

La Autoridad de Aplicación podrá imponer **medidas correctivas, sanciones administrativas** (como multas , suspensión temporal de actividades o cierre temporal) u obligar a que quien trate el dato realice efectivo cumplimiento de los derechos, estos últimos pueden interponer recursos de reconsideración ante dicha Autoridad.

Respecto de las **multas**, establece criterios para su fijación con unidades móviles (UM) y porcentaje de facturación anual global. Esas unidades móviles se actualizarán anualmente de acuerdo al Índice de Precios al Consumidor (IPC). Asimismo, amplía los criterios para graduar los valores teniendo en cuenta el tipo de dato, riesgo y posición económica del infractor.

TRANSFERENCIAS INTERNACIONALES.

Autoriza las transferencias internacionales tanto para el sector público como para el privado, siempre que se lo haga con **protecciones adecuadas**.

DEBERES DEL RESPONSABLE.

El Responsable del tratamiento de datos puede ser una persona física o jurídica. Estos, deben implementar todas las medidas tendientes a **garantizar el pleno ejercicio de los derechos de los titulares** de los datos, **brindar información adecuada y veraz**, **tratar a los datos de forma segura**, implementar medidas para que se mantengan actualizados y sean veraces. Son **responsables solidarios** por el tratamiento que hagan los Encargados o quienes subcontraten los servicios de tratamiento. Además, deben designar a una persona o área que asuma la función de **Delegado de Protección de Datos Personales**.

También incorpora el concepto de **Seguridad por Diseño/por Defecto**, es decir que el tratamiento de datos personales sea lo más seguro posible de manera tecnológica y organizativamente apropiada. Y crea un **Registro Nacional para la Protección de Datos Personales**, en donde deberán registrarse todos los Responsables y Encargados del tratamiento de datos.

## III. LO “MEJORABLE”.

Distintos especialistas en la materia han detectado falencias, entre ellas:

- ➔ En cuanto al catálogo de definiciones no se incluyen, por ejemplo, conceptos como “Nube”, “Exportador” e “Importador” de datos, que son términos que aparecen a lo largo del articulado y al no estar definidos claramente, pueden dar lugar a conflictos de interpretación.
- ➔ Se ha planteado que, si bien protege datos de titulares argentinos sin importar donde están alojados dichos datos, no especifica el tratamiento que se le debe dar a esos datos alojados fuera del país.
- ➔ Por otra parte, establece la aplicación de la ley a cualquier tratamiento de datos aplicando el Principio de Neutralidad Tecnológica, principio que en la práctica no se respeta.
- ➔ Respecto de la finalidad de recolección de datos estipula “(...) sólo se podrán archivar, registrar o ceder los datos personales que *sean significativos* para evaluar la solvencia económico-financiera de los afectados, durante los últimos 5 años (...)” artículo que al no especificar, abarca todo tipo de dato, es decir, es un artículo excesivamente abierto.
- ➔ También establece la responsabilidad del Titular de cumplir con el Principio de Exactitud de los datos que brinde, los cuales deben ser exactos, veraces, completos, comprobados y actualizados, pero, en la práctica, hay plataformas que no permiten la actualización y otras por las cuales cualquiera puede declarar datos falsos.

- ➔ No establece diferencias entre bajas físicas y bajas lógicas.
- ➔ Ante el pedido de supresión de un dato personal, la persona debe recurrir a asesoría o representación legal la cual, a su vez, debe concurrir a cada medio, servidor y almacenamiento que replica el dato, lo cual es engorroso o poco práctico.
- ➔ Establece la responsabilidad del Responsable o Encargado individualizándola en cabeza de una persona, cuando, en la práctica, recae sobre equipos de personas.
- ➔ En cuanto al consentimiento, en la práctica se dan innumerables casos en los que el titular no puede acceder a páginas o descargar aplicaciones sin adherirse a las extensas y complejas bases y condiciones.
- ➔ Establece que se le debe brindar al titular información sobre nombre/razón social/medios electrónicos del Responsable o Encargado, lo cual los expone si son personas físicas.
- ➔ También establece la prohibición, a los prestadores de salud del sector privado, de utilizar datos para selección de riesgo o exclusión de beneficiarios pero sin hacerla extensiva a laboratorios, farmacéuticas, etc. Exceptúa de esta prohibición a los casos en que se traten datos necesarios para el reconocimiento, ejercicio o defensa de derechos dentro de un proceso judicial, tengan finalidad histórica, archivo de interés público, estadístico o científico, lo cual es muy amplio y subjetivo.
- ➔ Además, nada se dice sobre los datos que recolecta la Iglesia.
- ➔ En cuanto al tratamiento de datos en el sector privado, no establece la responsabilidad compartida en el caso de cesiones de datos como en el sector público.
- ➔ No se expresa sobre el tratamiento de datos de personas argentinas, especialmente del sector público, en centros de datos extranjeros.
- ➔ Establece que los exportadores de datos deben cooperar con la Autoridad de Aplicación, lo cual en la práctica no ocurre. Inclusive, los contratos sobre transferencias internacionales de datos suelen quedar sujetos a jurisdicciones diferentes a aquellas donde se encuentran los servidores.
- ➔ Tampoco especifica la responsabilidad de progenitores en cuanto a datos que publiquen de sus hijos menores de edad, ni se expide sobre *grooming* o *ciberacoso*, *cyberbullying*.
- ➔ No menciona a las APIs[4].
- ➔ La figura del Delegado de Protección de datos Personales, es prácticamente inaplicable en pymes ya que implica, al menos, una inversión que impactará en su economía.
- ➔ La seguridad por defecto debería incluir la trazabilidad.
- ➔ Se dedica un capítulo entero a regular el Habeas Data, siendo que ya existe una ley para ello, la Ley 25.326, produciendo redundancia normativa.
- ➔ Se inmiscuye en cuestiones procesales, siendo una ley de fondo.
- ➔ No sigue los lineamientos de redacción conforme a la Guía para una comunicación con perspectiva de género del Ministerio de las Mujeres, Géneros y Diversidad.[5]

---

[4] Las APIs (*Application programming interface* o interfaz de programación de aplicaciones) son métodos de programación que ofrecen bibliotecas para que puedan ser utilizadas por otros softwares como capas de abstracción (es decir, como una forma de ocultar detalles de implementación de ciertas funcionalidades) por ello permiten la interoperabilidad de los datos.

[5]Para la producción del actual artículo, me basé en las lecturas de diferentes artículos de opinión especializada, tales como: "*Minucioso análisis del real cumplimiento de la propuesta de anteproyecto de la Ley de Datos Personales en el ámbito público como privado*", de Marcos Manssueti (https://www.linkedin.com/pulse/minucioso-an%C3%A1lisis-del-real-cumplimiento-de-la-ley-datos-mansueti ); "*La imperiosa necesidad de actualizar la Ley de Protección de Datos Personales de Argentina"* de M. Emilia Minuto (https://abogados.com.ar/el-futuro-llego-hace-rato-la-imperiosa-necesidad-de-actualizar-la-ley-de-proteccion-de-datos-personales-de-argentina/28139 ); "*Datos para cuidar*" y "*La reforma es todo un dato*"de Diario Judicial (https://www.diariojudicial.com/nota/93000; https://www.diariojudicial.com/nota/93058 ) ; "*Proceso de reforma del régimen de protección de datos personales*" de Mariano Peruzzotti (https://abogados.com.ar/argentina-reinicia-el-proceso-de-reforma-del-regimen-de-proteccion-de-datos-personales/31243 ).