



# Comentario sobre el Anteproyecto de Reforma de la Ley de Protección de Datos Personales

Proceso de Consulta Pública – Agencia de Acceso a la Información Pública – Jefatura de Gabinete de Ministros de la Nación

Contribución de Fundación Vía Libre

[www.vialibre.org.ar](http://www.vialibre.org.ar)

[info@vialibre.org.ar](mailto:info@vialibre.org.ar)

La iniciativa de actualizar la legislación sobre protección de datos personales, materializada en el Anteproyecto, satisface la evidente necesidad de conferir un mayor nivel de garantías sobre derechos personalísimos a la luz de la evolución tecnológica y jurídica habida desde la sanción de la ley 25326 y corregir las fallas observadas en la aplicación de esta. El Anteproyecto contiene muchos avances positivos para el fortalecimiento de los derechos de autodeterminación informacional, y representa una mejora significativa respecto del proyecto que el Poder Ejecutivo remitiera al Congreso en 2018.

Desafortunadamente, el período de consulta pública establecido por la Resolución AAIP 119/2022 es demasiado breve para llevar a cabo el análisis exhaustivo que una norma de esta importancia amerita. No obstante ello, y sin perjuicio de mantener abierto el intercambio de puntos de vista y observaciones sobre la cuestión, este documento sintetiza a grandes rasgos nuestros comentarios sobre el Anteproyecto. Más que concentrarse en el análisis detallado del articulado de la norma propuesta, este documento plantea observaciones y comentarios temáticos que, a nuestro juicio, pueden afectar los derechos que se procura proteger o entorpecer la operatividad de la norma.

## Protección de información personal como derecho fundamental

Parecería conveniente que el Anteproyecto destacara que los derechos sobre la información personal pertenecen a la categoría de los derechos personalísimos (Cfr. Artículo 1). Ello se deduce de la concepción doctrinaria generalmente aceptada sobre estos derechos, y por el sentido general del Título I, Capítulo 3 del Código Civil y Comercial de la Nación. Ese mismo artículo 1 hace mención a la “autodeterminación informativa”. Allí resultaría necesario

[www.vialibre.org.ar](http://www.vialibre.org.ar)  
[info@vialibre.org.ar](mailto:info@vialibre.org.ar)

introducir correcciones: por un lado, respecto del término empleado;<sup>1</sup> por otro, en el sentido que la autodeterminación informacional está fuertemente ligada a la protección de los datos personales pero se extiende más allá, como el derecho fundamental de las personas a decidir, con base en la autodeterminación, qué información sobre sí mismas es comunicada a los demás y bajo qué circunstancias y limitaciones, incluyendo por lo tanto áreas comunes con el derecho a la libertad de opinión y expresión, a la vida privada activa, a la protección de la privacidad, etc.<sup>2</sup>

## Definiciones

Una de las falencias del Anteproyecto reside en las definiciones. Las incluidas en el artículo 2 son insuficientes y en algunos casos ambiguas o técnicamente incorrectas. Debería considerarse la posibilidad de extender dichas definiciones en un anexo que forme parte integrante de la ley, y adaptar en cuanto fuera posible las de la sección 1798.140 del Código Civil del estado de California.<sup>3</sup> Por ejemplo, la definición de “anonimización” es problemática, y estaría mejor basada en una definición canónica de “anónimato”<sup>4</sup> como “el proceso técnico de volver anónimo un dato o un conjunto de ellos”; la definición de “dato genético” ha quedado limitada a la del artículo 4 del Reglamento General de Protección de Datos de la Unión Europea (Reglamento 2016/679) cuando sería preferible una más extensa como la del considerando 34 del propio Reglamento 2016/679.<sup>5</sup>

## Exclusiones

El artículo 3 del Anteproyecto excluye de los alcances de la ley a la información para uso exclusivamente privado, en consonancia con prácticamente la totalidad de la legislación comparada. Ahora bien, dado que la definición de “tratamiento de datos” incluye “comunicaciones, consultas, interconexiones o transferencias” (cfr. artículo 2) inclusive cuando los datos tratados “no formen parte de una base de datos” (cfr. primer párrafo del

- 1 El término procede del alemán *informationelle Selbstbestimmung* y se remonta a un dictamen de los juristas Wilhelm Steinmüller, Bernd Lutterbeck y otros (*Grundfragen des Datenschutzes*, realizado a requerimiento del Ministerio Federal del Interior alemán en 1971) y luego ampliamente conocido a partir del fallo “Censo” del Tribunal Constitucional Federal alemán ( BVerfG, *Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -*, Rn. 1-215). Se ha traducido en algunos casos como “autodeterminación informativa” pero en el caso “informativa” es antisemántico, pues no se trata de algo que informa (*informativ*) sino de algo relativo a la información. Si “autodeterminación informacional” se considerara inadecuado, puede emplearse la expresión “autodeterminación sobre la información personal”.
- 2 Cfr. Serge Gutwirth, Yves Poullet, Paul Hert, Cécile Terwangne, Sjaak Nouwt (eds.). 2009. *Reinventing Data Protection*. Dordrecht: Springer Netherlands.
- 3 Incorporadas por la California Consumer Privacy Act of 2018.
- 4 Puede adoptarse la de Andreas Pfitzmann y Marit Hansen. 2010. *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*. V0.34. Dresden: TU Dresden.
- 5 O bien la de la sección 1798.29(h)(5) del Código Civil de California.

artículo 3) sería de rigor establecer también una exclusión para los prestadores de servicios de comunicaciones que ejecutan esas operaciones en tanto estas se limiten a las acciones técnicamente necesarias para el transporte de dichos datos (“mero tránsito”).

En tanto la libertad de prensa constituye uno de los principios fundamentales de un Estado de Derecho, es razonable que no apliquen algunas previsiones relativas a la protección de los datos personales cuando puedan resultar colisiones. Sin embargo, esto no debe dar carta blanca para el tratamiento; garantizando la protección de las fuentes, resulta también necesario proteger los derechos de los titulares de los datos. En la legislación comparada esto se ha materializado en previsiones en la ley (por ejemplo, los casos en que se permite limitar el derecho de acceso de los titulares especificados en el artículo 27 de la nueva ley federal suiza) o mediante normas específicas dictadas por la autoridad de aplicación (*Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica* del *Garante per la protezione dei dati personali* italiano). Cualquiera sea la solución adoptada, resulta necesario establecer este equilibrio de derechos.

## Flujos transfronterizos de datos personales

La transferencia transfronteriza de datos ha sido generalmente bien resuelta en el Anteproyecto, pero caben allí algunas observaciones, a saber:

- Debería establecerse un criterio de reciprocidad de modo tal que si la transferencia de datos desde algún estado hacia la República Argentina fuera impedida o limitada sea posible adoptar medidas equivalentes respecto de las transferencias hacia ese estado.
- En el mismo sentido, debería preverse que cuando organizaciones o individuos extranjeros traten información personal de modo que viole los derechos e intereses de los residentes en la República Argentina o perjudique la seguridad o la defensa nacional se faculte al órgano de aplicación a emitir advertencias y, en casos más graves, limitar o prohibir el suministro de información personal con destino a los países donde residan esas organizaciones o individuos.

## Datos sensibles

En el tratamiento de datos sensibles:

- Debería suprimirse la salvedad del inciso a) del artículo 16, por excesivamente general, en tanto las restantes previsiones del texto cubren o deberían cubrir las circunstancias excepcionales para omitir el consentimiento.
- Debería eliminarse el inciso h) del artículo 16, de carácter demasiado vago y sujeto a la posibilidad de existencia de otra legislación que anule completamente los propósitos de protección de la información personal sensible enunciados en el Anteproyecto.
- Si se incorpora una excepción general al consentimiento para responder a sucesos repentinos de salud pública o para proteger la vida y la salud de las personas humanas

o la seguridad de sus bienes, en condiciones de emergencia, y siempre y cuando una vez cesada la emergencia se eliminen los datos o se obtenga el debido consentimiento o se practiquen las notificaciones requeridas, el tratamiento de datos sensibles por “razones humanitarias” (inciso i) del artículo 16) debería eliminarse. El carácter amplio de las “razones humanitarias” puede conducir a excesos.

- Debe analizarse la conveniencia de determinar un marco restringido para la transferencia internacional de datos sensibles.

## Adolescentes

Respecto de las personas menores de edad, y teniendo en cuenta la categorización de ejercicio progresivo de los derechos que surge del artículo 26 del Código Civil y Comercial de la Nación, parece necesario extender y explicitar el criterio propuesto en el Anteproyecto. Así pues, las personas adolescentes no solo deben tener capacidad para consentir, sino también para retirar el consentimiento que fuera otorgado por los titulares de la autoridad parental. En contrapartida, los titulares de la autoridad parental deberían tener la capacidad de retirar el consentimiento otorgado por adolescentes en la franja de 13 a 16 años (y en la franja de 16 a 18 si ese consentimiento implicara afectación patrimonial). La ley debería también establecer quiénes son sujetos activos en el ejercicio de los derechos que la ley otorga a las personas titulares; parece razonable que esta facultad se otorgue a las personas mayores de 16 años sin obstar a la concurrencia de las titulares de la autoridad parental.

## Imágenes

Las imágenes tomadas en público o en lugares de acceso público irrestricto,<sup>6</sup> en tanto susceptibles de tratamiento de datos y dado su carácter de datos sensibles, solo pueden ser procesadas con fines de seguridad pública. Si bien resulta conveniente regular el empleo de cámaras y otros dispositivos de observación en estos espacios, parece aconsejable por razones prácticas que dicha regulación sea desplazada al tratamiento de una ley más general sobre privacidad (en particular, privacidad en los contextos digitales o “*e-privacy*”).

## Inferencia y derecho a la explicación

Si bien un volumen significativo de datos personales son recolectados por mecanismos de observación y captación, ya sea obtenidos directamente de las personas titulares o a través de otras fuentes, no es menos significativo el volumen de datos que son inferidos por los

---

<sup>6</sup> Los lugares de acceso público irrestricto incluyen aquellos en que la condición de acceso solo está limitada al pago de una entrada o canon similar.

responsables de tratamiento. En términos no rigurosos, estas inferencias siguen la lógica de que si la persona P tiene los atributos  $p_1, \dots, p_n$  existe una cierta probabilidad de que tenga (o no tenga) un cierto atributo  $p_i$  no observado (por ejemplo, la propensión a adquirir ciertos bienes o servicios, o —con consecuencias más graves para la privacidad— que tenga una determinada condición de salud). Es necesario que la ley limite las inferencias para evitar tratamientos abusivos y garantice que el derecho de acceso de las personas titulares comprende el acceso a los datos inferidos, con explicación de su significado y de los procesos mediante los cuales fueron construidos y el ejercicio respecto de ellos de los demás derechos que la ley otorga.

El Anteproyecto restringe el derecho de acceso relativo a las decisiones automatizadas cuando la explicación de la lógica de la decisión “afecte derechos intelectuales del Responsable del tratamiento”. Esta previsión debe ser suprimida, porque en cualquier caso los derechos personalísimos priman sobre un mero derecho patrimonial como la propiedad intelectual. De hecho, la regla general debería ser que no pueden llevarse a cabo decisiones automáticas, inferencias o identificaciones probabilísticas que sean resultado de un proceso que no puede ser explicado a la persona titular de los datos de modo tal que esta pueda razonablemente comprender cómo se arribó al dato en cuestión. En otros términos, la regla para los responsables de tratamiento puede expresarse como “si no puede explicarlo no puede hacerlo”.

## Normas penales y procedimentales

La ampliación de garantías respecto de los datos personales implica también que el espectro de su vulneración puede ser más amplio. De allí puede surgir que sea necesario penalizar conductas hasta ahora no contempladas,<sup>7</sup> por lo que resultaría de utilidad una revisión de este aspecto antes de que el proyecto sea elevado al Congreso.

Una serie de cuestiones procedimentales que deberían estar contempladas en la ley:

- Cuando la autoridad administrativa resuelva un caso en favor de la pretensión del titular de los datos, la eventual apelación en sede judicial tendrá efecto devolutivo.
- Las personas sancionadas por infracciones a la ley no podrán ejercer funciones de delegado de protección de datos por el período que se establezca en la propia sanción, que podrá ser permanente.
- Cuando se instruya una causa relativa a infracciones a las normas penales sobre datos personales, el Ministerio Público deberá notificar a la autoridad de aplicación y esta, si decidiera intervenir, tendrá legitimación como querellante.

---

7 Véanse, por ejemplo, los artículos 226-16 a 226-24 del Código Penal francés.

## Autoridad de aplicación

La autoridad de aplicación debe estar facultada para dictar normas de cumplimiento obligatorio, y contar con los poderes suficientes para hacerlas observar. Estas normas incluyen, a título puramente enumerativo:

- Condiciones de seguridad exigidas para el tratamiento de datos sensibles (por ejemplo, que los datos sensibles se almacenen siempre en forma cifrada);
- Normas para el tratamiento de datos personales en circunstancias de excepción del consentimiento, en particular:
  - Archivos
  - Investigación y defensa de derechos en sede judicial
  - Estadísticas e investigación científica<sup>8</sup>
  - Actividad periodística
- Protocolos de inspección de las instalaciones y documentación de los responsables y encargados de tratamiento

La autoridad de aplicación, como se señala más arriba, debe tener capacidad suficiente para hacer cumplir la ley. Esto así en dos sentidos: legal y operativo. En el primer sentido, es necesario dotar a la autoridad de aplicación de potestades para requerir cualquier información necesaria y para ingresar a cualquier local en que se efectúe tratamiento de datos sin necesidad de previa orden de allanamiento; al mismo tiempo, dado que en uso de esas facultades el personal de la autoridad de aplicación podría entrar en conocimiento de información de carácter secreto, estas personas deben estar obligadas por normas de confidencialidad que se prolonguen más allá de la finalización de su relación con la autoridad. En sentido operativo, la autoridad de aplicación debe contar con los recursos humanos, técnicos y financieros necesarios para el cumplimiento de su cometido.

La protección de los datos personales no solo requiere de una ley. Para cumplirla efectivamente es indispensable que el órgano encargado de aplicarla sea apto para el cometido. Sin perjuicio de las condiciones señaladas en el párrafo anterior, resulta claro que no es posible un cumplimiento efectivo sin que la autoridad de aplicación tenga condiciones de independencia y profesionalidad. Ello exige la selección de la autoridad por la vía de mayor transparencia posible, de modo que las personas a cargo de dirigir este organismo resulten efectivamente las más capacitadas para la función.

A nuestro entender, colocar la responsabilidad de la protección de datos personales en cabeza de la actual Agencia de Acceso a la Información Pública es contrario a los principios señalados más arriba. En efecto, cuando la selección de la autoridad está al arbitrio del Ejecutivo (cabe recordar que el procedimiento establecido en el artículo 21 de la ley 27275 no otorga carácter vinculante a los resultados de la audiencia pública) y no se exige que la persona titular de esa Agencia tenga experiencia o conocimientos sobre protección de datos

---

8 La ley italiana (*Codice in materia di protezione dei dati personali*) distingue entre los fines estadísticos y de investigación científica en general y los del sistema científico estatal.



Fundación  
Vía Libre

personales, no hay ninguna garantía efectiva de que se de cumplimiento a la misión específica más allá de la buena voluntad de quien ocupe la dirección de la Agencia. Parece indispensable por un lado garantizar que quien (o quienes, en el caso de un cuerpo colegiado) sean responsables por la autoridad de aplicación surjan de concurso público y abierto de oposición y antecedentes, evaluado por una comisión ad-hoc del Congreso, y cuenten con el aval de este. El proceso que llevó a la constitución de la Defensora de los Derechos de Niños, Niñas y Adolescentes (artículo 47 y ss. de la ley 26061) puede servir de referencia al respecto.