RCCyC

REVISTA CÓDIGO CIVIL Y COMERCIAL

FAMILIAS • OBLIGACIONES • INSOLVENCIA

Dirigida por **Héctor Alegria** y **Graciela Medina**

Año VIII | Número 2 | Abril 2022

ISSN 2469-049X

INCLUYE VERSIÓN DIGITAL

THOMSON REUTERS
LA LEY

Régimen argentino de protección de datos personales

Marina Basavilbaso (*)

Sumario: I. Introducción. Un breve repaso histórico.— II. Apuntes iniciales sobre la protección de datos personales en el ordenamiento jurídico argentino.— III. El caso particular de los datos sensibles.— IV. Conclusión.

I. Introducción. Un breve repaso histórico

En ocasión de esta edición de la revista del Cód. Civ. y Com. me propuse hacer un repaso del régimen argentino de protección de datos personales. El objetivo de este artículo es proporcionar a quienes no conozcan cómo nuestro ordenamiento regula el procesamiento de datos personales una primera aproximación a la materia.

Si bien la protección de la privacidad tiene orígenes mucho más antiguos, las primeras regulaciones en materia de procesamiento de datos personales como hoy las conocemos surgieron en Europa en los años setenta a raíz de la proliferación de los entonces llamados "ficheros automáticos". Una década más tarde, en enero de 1982 el Consejo de Europa firmó el *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* (en adelante, el "Convenio 108"), que sentó las bases de las regulaciones modernas. El Convenio 108 reconoció la necesidad de que los países miembros procuraran una regulación uniforme para garantizar a nivel regional una protección homogénea de los datos personales a través del cumplimiento obligatorio de los siguientes principios básicos que siguen siendo hoy los principios que rigen esta materia:

1. Licitud: los datos personales deben obtenerse de manera legítima y procesarse con finalidades lícitas. Deben ser exactos y estar actualizados, y deben conservarse durante un tiempo que sea razonable en relación con la finalidad para la que fueron obtenidos.

2. Los datos sensibles **(1)** merecen un tratamiento especial y solo deben procesarse cuando estén garantizadas las medidas de seguridad adecuadas para protegerlos con mayor nivel de cuidado.

3. El procesador debe tomar las medidas de seguridad necesarias para proteger los datos procesados.

4. Toda persona tiene derecho a saber que sus datos están siendo procesados, y debe gozar de los derechos de acceso, rectificación y supresión.

Además, el Convenio 108 sentó las bases para lo que en su momento se denominó el "flujo transfronterizo de datos", cuestión que hoy en día sigue siendo una de las más debatidas en materia de privacidad. Ya entonces se prohibía limitar o someter a autorización el flujo libre de datos personales entre los Estados Miembros (con excepciones), aunque no se prohibía ni limitaba el flujo con terceros países como sí ocurrió más adelante.

(*) Abogada por la UCA, promoción 2013. Realizó el Máster en Derecho Empresario de la Universidad Austral y el Posgrado en Derecho Internacional Comparado en la Southwestern Institute of Dallas en Texas, EE. UU. Es consejera de Pérez Alati, Grondona, Benites & Arntsen, especialista en Derecho de la Tecnología, Medios y Telecomunicaciones, así como en Datos Personales.

(1) El art. 7 del Convenio 108 en aquel momento ya consideraba que eran datos sensibles aquellos que "revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual".

De allí a esta parte surgieron en Europa numerosas leyes nacionales y normas regionales, hasta llegar al ya conocido Reglamento General de Protección de Datos Personales de la Unión Europea (Reglamento 2016/679) que se aprobó en 2016, entró en vigencia en mayo de 2018 y que volvió a sacudir el tablero, esta vez causando un impacto grande, que fue mucho más allá de las fronteras de Europa (en adelante, el "Reglamento Europeo de Privacidad").

En nuestra región, el surgimiento de las leyes de privacidad se dio a fines de los años noventa de la mano de la primera ley brasilera de protección de datos personales aprobada en 1997. En Argentina, la Ley Nacional de Protección de Datos Personales 25.326 (en adelante la "LNPDP" o la "ley") fue aprobada en el año 2000, y su Decreto Reglamentario 1558/2001 en 2001, y si bien fue bastante pionera en su momento, no ha sufrido modificaciones sustanciales desde entonces. Si uno considera que el procesamiento de datos personales se realiza prácticamente en su totalidad a través de medios tecnológicos, y que grandes plataformas tecnológicas de la actualidad están basadas en el procesamiento masivo de datos, fácilmente puede inferir que una ley con 22 años de antigüedad ha quedado definitivamente desactualizada. Naturalmente, la LNPDP tiene normas que la complementan y en cierto punto la han ido modernizando, pero eso no ha suplido la necesidad de una actualización más profunda y sistemática, que replantee cuestiones relevantes, y descarte algunas regulaciones antiguas que ya no tienen razón de ser.

Entre las normas que han complementado y modernizado nuestro régimen recientemente destacamos (y celebramos) la importancia de la aprobación en 2016 de la ley 27.275 de Acceso a la Información Pública (la "Ley de Acceso a la Información Pública"). Como el nombre lo indica, el objeto de esta ley está acotado a la información que está en manos del Estado, pero esto no le quita relevancia, ya que, si bien en los últimos años el foco se ha puesto en el procesamiento por parte de instituciones privadas, el Estado es el más grande de los procesadores de datos. Además, la Ley de Acceso a la Información Pública creó la Agencia de Acceso a la Información Pública (la "AAIP", la "Agencia" o la "Autoridad de Control") y le dio a la autoridad de control de la LNPDP autarquía, cuestión que es sumamente relevante para que la Argentina siga siendo calificada como país seguro por el Comité Europeo de Protección de Datos.

Además de la Ley de Acceso a la Información Pública, aunque en menor medida, son también relevantes la res. AAIP 47/2018 con recomendaciones de seguridad; la res. AAIP 4/2019 con criterios orientadores e indicadores de mejores prácticas; y por su relevancia para facilitar la transferencia internacional de datos, la disp. DNPDP 60/2016, y la res. AAIP 159/2018.

Por otro lado, en los últimos años se ingresó más de un proyecto de ley para modificar la LNPDP, entre esos proyectos se destaca el proyecto que ingresó el entonces presidente de la Nación Mauricio Macri en septiembre de 2018 (el "Proyecto de Reforma"). Aquel proyecto buscaba modificar de manera íntegra la LNPDP y recogía de buena manera la mayor parte de las actualizaciones en la materia introducidas en Europa por el Reglamento Europeo de Privacidad. Lamentablemente dicho proyecto no prosperó y al día de hoy sigue pendiente una actualización que confiamos llegará más pronto que tarde.

II. Apuntes iniciales sobre la protección de datos personales en el ordenamiento jurídico argentino

Hoy, a cuarenta y un años de la firma del Convenio 108, podemos decir con confianza que en nuestro ordenamiento jurídico casi toda la información está protegida de alguna manera. La LNPDP define "datos personales" como: "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". La definición es sin duda muy amplia, de hecho, incluye la información de personas jurídicas, cosa que no es habitual en las regulaciones más modernas. Además, el hecho de que se incluya a las personas "determinables" implica que, aunque cierta información no esté inicialmente relacionada con una persona, si el dato y su titular pueden asociarse —aunque para ello haya que implementar una serie de mecanismos o esfuerzos— la información en cuestión será considerada y protegida como dato personal.

Los datos personales de una persona van desde su información más básica como el nombre, la edad o el sexo, hasta sus datos más sensibles como la religión que profesa, su afiliación política o gremial, entre tantos otros. Entonces, en definitiva, todo lo que es, hace, dice o profesa una persona es información personal suya y constituye un bien jurídico protegido por esta ley nacional de orden público y tratados internacionales. Además, la ley abarca todo tipo de procesamiento, tanto el realizado por personas públicas como privadas. Solo parece quedar afuera del alcance de la ley el procesamiento que hacen las personas físicas para su uso personal, y la información que se procesa completamente disociada.

Pero ¿de qué exactamente nos protege la LNPDP, cómo se protege la privacidad y qué derechos otorga?

Como la información es intangible y se puede reproducir sin límites, durante mucho tiempo, la información personal de todos estuvo, de alguna manera a disposición de todos. Bastaba con tener acceso a la información de alguien para pasar a ser "dueño" de esa información obtenida y poder reproducirla, compartirla, analizarla, asociarla con otra información, etc. Sin embargo, a partir del surgimiento de las normas de privacidad la información personal pasó a ser un bien jurídico protegido, y hoy nadie puede acceder, usar, procesar, ceder o almacenar (entre otras acciones reguladas) información personal sin el consentimiento de su titular, y en caso de que alguien intente hacerlo o lo haga, existen herramientas jurídicas para impedirlo o detenerlo.

A continuación, se enumeran los requisitos que debe cumplir un procesamiento de datos para que este pueda ser considerado lícito.

II.1. El consentimiento

El procesamiento debe ser consentido por el titular de los datos, salvo en los casos en los que la LNPDP prevé expresamente que el consentimiento no es necesario.

El consentimiento que brinda el titular de los datos a procesar debe ser expreso, libre e informado. Según la LNPDP el consentimiento no es necesario cuando: (i) los datos se obtengan de fuentes de acceso público irrestricto; (ii) se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal (iii) se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; (iv) deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; y (v) se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del art. 39 de la ley 21.526 de Entidades Financieras.

Estas excepciones deben ser aplicadas de manera restrictiva **(2)** y en la práctica el consentimiento generalmente se recaba a través de la aceptación de términos y condiciones de uso, contratos de adhesión a servicios o programas o cuestiones similares, ya que la expresión del consentimiento debe ser precedida de la información mínima con la que debe contar el titular del dato para poder consentir el procesamiento **(3)**.

II.2. La finalidad

La finalidad con la que se procesan los datos debe ser informada y consentida por el titular, pero además no puede ser contraria a las leyes o a la moral pública. Si bien este requisito no había dado mucho de qué hablar, ha tomado mayor protagonismo en los últimos años con el caso de Cambridge Analytica y la entrada en vigencia del Reglamento Europeo de Privacidad que ha incorporado entre los llamados "nuevos principios" el principio de la limitación de la finalidad. Este principio prevé que "[l]os datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines (...)" y prevé que los fines explícitos y legítimos deberán determinarse en el momento de la recogida de los datos.

II.3. Registración de las bases de datos

El art. 3° de la LNPDP prevé: "La formación de archivos de datos será lícita cuando se encuen-

(2) "Torres Abad, Carmen c. EN-JMG s/ habeas data".

(3) Ver art. 6 LNPDP.

tren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia".

Este es uno de los ejemplos que con más claridad evidencia la vejez de nuestra LNPDP. Según lo establece la norma, toda persona física o jurídica **(4)** debería registrar todos sus archivos o bases de datos en el Registro Nacional de Bases de Datos. Al momento del surgimiento de la ley, eran menos frecuentes los "bancos de datos" y la LNPDP buscó con este requisito tener bajo control a aquellos que se dedicaran a generar ficheros o bancos de datos, para asegurar el cumplimiento de la normativa. Sin embargo, hoy sería imposible registrar y mantener actualizado un registro nacional con todas las bases de datos que constantemente se crean, actualizan y eliminan.

Sabemos que la AAIP abogó hace algunos años por la supresión de este requisito legal, de hecho, el Proyecto de Reforma preveía abandonar este requisito por considerar que "la experiencia ha demostrado poco útil, y cuyo cumplimiento no ha sido del todo adecuado". Como la eliminación no se terminó concretando, se optó por modernizar el registro para que el ahora llamado "empadronamiento" se realice únicamente una única vez, salvo modificaciones sustanciales a las bases registradas. Téngase presente que hasta el año 2018 era necesario hacer una presentación anual en papel con firma certificada por escribano público por cada base de datos que tuviera una compañía. Además, hoy la Agencia solo exige formalmente el registro de las bases de datos de empleados, de proveedores, de clientes y de cámaras de videovigilancia (asumiendo que esas bases existen necesariamente). Tampoco podemos dejar de mencionar que esta exigencia de la ley ha sido perseguida en ocasiones muy excepcionales, y que el incumplimiento ha sido únicamente sancionado (hasta donde tenemos conocimiento) en casos en los que antes había sido formalmente exigido por la autoridad.

En pocas palabras, esta sigue siendo una exigencia de la ley que ha quedado muy desactualizada por haber perdido su razón de ser y que esperamos pronto sea eliminada.

II.4. Confidencialidad y seguridad

La LNPDP prevé: "El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos".

El deber de confidencialidad naturalmente puede ser relevado por orden judicial y cuando medien razones fundadas en la seguridad pública.

Para poder cumplir con este requisito de confidencialidad es necesario que el responsable arbitre todos los medios "técnicos y organizativos" que sean razonables para poder asegurar la confidencialidad de los datos. Este requisito genérico fue regulado con mayor detalle recientemente a través de la res. AAIP 47/2018 a través de la cual la Autoridad de Control dispuso una serie de medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y no informatizados. Téngase presente que según lo dispone la propia res. 47, dichas medidas son recomendaciones y no han sido dispuestas como obligaciones por la autoridad.

Entre las medidas de seguridad recomendadas por la res. 47 antes mencionada merece una mención especial la recomendación de notificar a la AAIP en caso de un incidente de seguridad. Decimos que merece una mención especial porque los reportes de incidentes son obligatorios en muchas jurisdicciones y muchas instituciones los han adoptado como un uso de "mejores prácticas" para los países como el nuestro en el que no es exigido por la ley. Según la recomendación de la res. 47 el reporte debería realizarse por correo electrónico a la AAIP con información sobre el incidente y los protocolos aplicados. Si el incidente debe ser además reportado a los titulares de los datos es un tema aparte que merece un análisis más profundo, pero los deberes de cuidado y de no dañar establecidos en nuestro Cód. Civ. y Com. parecen inferir que en muchos casos es conveniente, sobre todo cuando el incidente pueda generar un

(4) Con excepción de aquellas bases de datos que se crean para el solo uso personal.

daño que puede ser mitigado por el titular si lo conoce a tiempo.

II.5. Derechos de información, acceso, rectificación y supresión

El procesamiento de datos en Argentina solo es legítimo si, además de cumplir con los requisitos enumerados en los párrafos precedentes, les otorga a los titulares de los datos los derechos de información, acceso, rectificación y supresión.

El derecho a la información está recogido en diferentes artículos de nuestra LNPDP, pero esencialmente consiste en que el titular de los datos siempre debe ser informado del hecho de que sus datos están siendo procesados, por quién están siendo procesados, dónde, cómo y para qué. Esta información debe brindarse siempre al titular de los datos cuyo consentimiento se recaba para el procesamiento.

Los derechos de acceso, rectificación y supresión son comúnmente conocidos como los derechos "ARCO" (por las siglas de acceso, rectificación, cancelación y oposición) y son internacionalmente reconocidos como los derechos básicos que tienen los titulares de datos personales. Tal como las denominaciones mismas lo infieren, consisten en el derecho de acceder a las bases de datos para conocer qué datos de uno se están tratando; rectificarlos en caso de que sean incorrectos o estén desactualizados; suprimirlos o cancelarlos en caso de que el titular quiera revocar el consentimiento que prestó para el consentimiento (o, por supuesto, que decida retirar sus datos de un banco que no le requirió su consentimiento en primer lugar); y oponerse al procesamiento.

Los derechos de acceso, rectificación y supresión deben ser anunciados al titular de los datos con claridad, y deben poder ser ejercidos de manera gratuita. La LNPDP prevé que el derecho de acceso se ejerza una vez cada seis meses como máximo, pero no prevé intervalos específicos para los derechos de rectificación y supresión, ya que estos deberían poder ser ejercidos en cualquier momento, cuando corresponda la actualización o se requiera la supresión.

Además, el responsable del procesamiento debe responder a los requerimientos de acceso dentro de un plazo de 10 días corridos, y a los requerimientos de rectificación y supresión dentro de un plazo de 5 días hábiles. Naturalmente, quien solicita el acceso, rectificación o supresión deberá demostrar su legitimidad a través de la exhibición de su documento nacional de identidad o a través de documentos que demuestren el vínculo o motivo que legitima la solicitud (por ejemplo, en el caso de padres que ejercen los derechos por sus hijos menores).

Si bien durante muchos años los derechos ARCO fueron considerados los derechos de privacidad por excelencia, el Reglamento Europeo de Privacidad introdujo los derechos que hoy se conocen como derechos de nueva generación, que no están recogidos por nuestro ordenamiento. Estos "nuevos derechos" son:

1) derecho a la transparencia;

2) derecho a la supresión **(5)**;

3) derecho de limitación; y

4) derecho a la portabilidad.

No haré un análisis de estos "nuevos derechos" ni de la conveniencia de recogerlos porque ello escapa el objeto de este análisis, pero sí parece conveniente introducir al lector respecto del hecho de que las normas más modernas han ido recogiendo nuevos derechos que, dependiendo de la coyuntura de cada país o región pueden resultar convenientes o no.

III. El caso particular de los datos sensibles

Habiendo hecho un breve repaso sobre el régimen general del procesamiento de datos personales en Argentina, me gustaría hacer un poco más de hincapié en la cuestión de los denominados datos sensibles.

(5) Téngase presente que lo que el texto en Castellano del Reglamento Europeo de Privacidad llama derecho de supresión no es lo mismo que lo que en nuestra ley se recoge con esa misma palabra. La LNPDP se refiere a la posibilidad de eliminar una información determinada de una base, mientras que el derecho a la supresión europeo se refiere al conocido como "Derecho al Olvido", no recogido por nuestra normativa e incluso rechazado por la jurisprudencia nacional en reiteradas ocasiones.

La LNPDP define datos sensibles como "[d]atos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". En las regulaciones más modernas, la definición de datos sensibles ha ido evolucionando hacia una definición más amplia, por ejemplo, en el Proyecto de Reforma se definía a los datos sensibles como "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". Sin embargo, más allá de las definiciones adoptadas, hoy todos coinciden en que los datos de salud y los datos que tienen la potencialidad de generar una discriminación de cualquier tipo deben ser protegidos como datos sensibles.

Pero lo que presenta un caso particular en nuestro ordenamiento no es la definición de datos sensibles, sino que según la LNPDP "[l]os datos sensibles solo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares". Es decir que en Argentina no basta con tener el consentimiento del titular del dato para poder procesar sus datos sensibles, sino que es necesario que una ley específicamente lo autorice.

Si bien la Autoridad de Aplicación se ha manifestado en algunos expedientes privados al hecho de que una interpretación armónica de la norma permitiría procesar datos sensibles con el consentimiento expreso de su titular, lo cierto es que la letra de la ley no lo autoriza y hacerlo entraña un riesgo que dependiendo del caso podrá ser calificado entre moderado y alto, pero que no se puede descartar.

El problema de que la ley no autorice expresamente a procesar datos sensibles en base al consentimiento de sus titulares es que, en muchos casos, el procesamiento de este tipo de datos es indispensable para el desarrollo de nuevos medicamentos, para mejorar tratamientos, para mejorar políticas de diversidad, etc. No parece tener mucho sentido que las personas que sufren una enfermedad determinada no puedan autorizar a una organización no médica a que procese sus datos para un estudio, o que personas que se consideran parte de una minoría no puedan autorizar a terceros a que recaben sus datos para mejorar políticas de diversidad en la institución en la que trabajan, por ejemplo.

Téngase presente que los datos sensibles sí pueden procesarse si están disociados de manera irreversible **(6)**, pero muchas veces la disociación empobrece u obstruye la calidad de los resultados de las investigaciones. Creo que en este aspecto debería adoptarse la modificación propuesta en el Proyecto de Reforma, que en su art. 16 preveía la legitimación del procesamiento de datos sensibles con base en el consentimiento de sus titulares.

IV. Conclusión

Para concluir, creo que definitivamente la Argentina es un país que puede seguir considerándose seguro en materia de privacidad, porque nuestra normativa, si bien es vieja y está desactualizada, tiene sentadas las bases para una protección sólida de los datos personales. Sin embargo, creo que deberían aprovecharse algunos proyectos de reforma que recogieron muy bien las tendencias internacionales más actuales para actualizar nuestra normativa y volver a ponernos a la altura de los países más modernos en materia de privacidad, como fuimos hasta hace pocos años.

(6) La Dra. CABRERA, María Laura en "La protección de datos sensibles en las investigaciones clínicas" publicado en la página web del Ministerio de Salud de la Nación distingue dos tipos de disociaciones que surgen de la ley: el primero es aquél en el que se preserva la identidad del titular [art. 11 inc. d)] pero el titular es eventualmente identificable por un grupo de personas (por ejemplo el médico a cargo de la recolección de un grupo de datos); y el segundo tipo de disociación es la disociación irreversible, en la que se han aplicado mecanismos que no permiten que el titular sea identificado por nadie.