Título: El futuro de la regulación en protección de datos personales en la Argentina
Autor: Faliero, Johanna Caterina
Publicado en: Sup. Esp. LegalTech 2018 (noviembre), 05/11/2018, 55
Cita Online: AR/DOC/2375/2018

(*)

I. Introducción

La protección de datos personales, como aquella disciplina jurídica tuitiva que se encarga de proteger los datos personale

s de los titulares, débil jurídico de la relación de tratamiento de datos frente al responsable de estos, con miras a la preservación de su derecho de autodeterminación informativa, representa en la actualidad, en nuestra era de datos, un punto regulatorio clave en las normativas regionales y locales de todo el mundo.

La tutela de los datos personales, no solo como un desprendimiento de un derecho personalísimo del individuo, sino también como una manifestación y extensión de la soberanía nacional, se sitúa como una de las preocupaciones cardinales en las agendas gubernamentales de los estados.

Desde una visión institucional u organizacional, la planificación estratégica en materia de gobierno de datos ya no constituye una actividad o área que se limita solo a aquellas organizaciones o instituciones de gran porte que trabajan con grandes volúmenes y flujos de datos. Hoy día, todo actor que trabaja con datos, es decir, que realiza tratamiento de datos personales, independientemente de su envergadura, debe velar por la protección, integridad y seguridad de, muy probablemente, el activo más valioso que posee.

Los datos en relación constituyen información, y la información en la era de datos es mercancía de intercambio. El flujo de datos, su tráfico y la producción de valor a través de su tratamiento constituyen la manifestación más ostensible de que nuestra moderna economía se encuentra sostenida en lo intangible.

Por otra parte, la protección de datos personales encuentra minuto a minuto nuevos desafíos, riesgos y daños posibles, así como vacíos e interrogantes regulatorios, frente al incontenible avance de las técnicas de procesamiento de datos, las que, al incrementar sus velocidades, volúmenes, complejidad y posibilidades, generan escenarios nuevos, en los que se debaten los derechos de los titulares de los datos, las necesidades de la industria de procesamiento de datos y la realidad del hecho técnico que, cada vez, demuestra ser más incontenible en sus consecuencias.

Efectuado este breve racconto introductorio, no resulta sorpresivo comprender el porqué de la necesidad basal de actualizar la normativa en protección de datos personales, puesto que no solo no regula un derecho y un objeto estático, sino que condiciona una realidad tecnológica que se encuentra en permanente evolución y crecimiento.

En el presente artículo se verá cómo se sitúa nuestro panorama regulatorio nacional frente a la reforma del actual régimen de protección de datos personales, cuál es el futuro de la regulación que se encuentra prevista en sustitución de la vigente y cómo se proyecta su impacto en esta área tan crítica de nuestra sociedad.

II. La protección de datos personales en la Argentina, la ley 25.326 y su proyecto de reforma

A modo de breve recorrido por nuestra evolución normativa, la primera regulación en materia de protección de datos personales en el sistema normativo argentino ha sido el juego del art. 33, protección de datos personales como un derecho implícito, art. 19 —principio de reserva— y art. 18 —inviolabilidad del domicilio, la correspondencia y los papeles privados— de nuestra Constitución Nacional, y por medio del art. 1071 bis del entonces Cód. Civil —Código Civil de la Nación Argentina velezano—, el que fuera reemplazado por el actual art. 1770 del Cód. Civ. y Com. —Código Civil y Comercial de la Nación Argentina—, por vía de la regulación del derecho a la intimidad.

Tiempo más tarde, con la Reforma Constitucional del año 1994, se incorporó a la Constitución Nacional el art. 43 que, en su párrafo tercero, introduce la figura del hábeas data, en el que se reconocen los derechos clásicos en materia de protección de datos, conocidos como "derechos ARCO" por los de acceso-rectificación-confidencialidad/cancelación-oposición.

Finalmente, la protección de datos personales en la Argentina recibe su regulación específica con la sanción de la ley 25.326, de Protección de los Datos Personales, reglamentada por el decreto 1558/2001.

El objeto de la Ley de Protección de Datos Personales 25.326 es amplio y referido a la actividad que representa el tratamiento de datos y focaliza su eje protectorio en el derecho humano fundamental de origen constitucional implícito, es decir, el de autodeterminación informativa.

La Ley de Protección de los Datos Personales 25.326 enuncia en su art. 1º (1) que tendrá por objeto la protección integral de los datos personales, mas no define per se qué es la protección integral de los datos personales (2).

La ley 25.326, sancionada el 4 de octubre del año 2000 y promulgada el 30 de octubre del mismo año, estableció el régimen de protección con disposiciones y principios generales, la enunciación acabada de los derechos de los titulares de los datos, derechos y deberes de los usuarios y responsables, el deber de inscripción de las bases de datos, su control, un sistema sancionatorio frente al incumplimiento de la norma y la regulación procedimental de la acción de protección de datos personales.

La ley 25.326 fue reglamentada por el decreto 1558/2001, modificado por el decreto 1160/2010. Su actual órgano de control, es decir, su autoridad de aplicación —la Agencia de Acceso a la Información Pública (3)— tiene como una de sus funciones el dictado de las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por la ley, conforme con el art. 29, inc. b).

Para ello, a lo largo de los años ha dictado numerosas disposiciones regulatorias en una pluralidad de temas relativos a la protección de datos personales (p. ej., normas registrales, régimen sancionatorio, regulaciones especiales, normas de inspección y control, guías de buenas prácticas, organización interna, registro nacional "no llame", etc.), disposiciones regulatorias que la misma autoridad de aplicación ha ido modificando progresivamente.

La Ley de Protección de Datos Personales actualmente se encuentra atravesando un proceso que tiene por objeto su reforma, que inicia en 2016. A estos fines y en el marco del Proyecto denominado Justicia 2020, creado por el Ministerio de Justicia y Derechos Humanos, durante el año 2016 se recibieron aportes de los más diversos y prestigiosos representantes de todos los sectores de la sociedad civil (sector privado, gobierno, academia, tercer sector) respecto de los puntos a reformar de la norma, a partir de los cuales se elaboró el documento "Ley de Protección de Datos Personales en Argentina. Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma. Agosto-Diciembre 2016"(4) de la entonces Dirección Nacional de Protección de Datos, ahora denominada Agencia de Acceso a la Información Pública.

En consonancia con estos aportes recibidos, se procedió a la redacción de una primera versión del Anteproyecto de Reforma de la Ley de Protección de Datos Personales (5), el que fuera publicado el 1 de febrero de 2017.

Luego de su publicación, y durante el transcurso de ese mismo mes, se recibieron nuevamente aportes críticos de los diversos representantes de todos los sectores de la sociedad civil, a partir de lo cual se elaboró una segunda versión de la redacción del Anteproyecto de Reforma de la Ley de Protección de Datos Personales (6).

De esta última versión y sus correcciones, se desprende el Proyecto de Reforma a la Ley de Protección de Datos Personales (7) que se envió el 19 de septiembre de 2018 al Congreso de la Nación, el que propone la derogación de la Ley de Protección de los Datos Personales 25.326, de su modificatoria 26.343 y de la ley 26.951, de creación, en el ámbito de la entonces Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos, hoy Agencia de Acceso a la Información Pública, organismo descentralizado en la órbita de la Jefatura de Gabinete de Ministros, del Registro Nacional "No Llame".

Si dicho Proyecto se aprueba conforme a su redacción, se establece en su art. 89, del mismo modo que se efectuó con la sanción y entrada en vigencia del nuevo marco regulatorio europeo, tal como se verá en el título que sigue, un plazo de dos años desde su publicación en el Boletín Oficial para la entrada en vigencia de las disposiciones de la nueva ley.

III. El impacto del nuevo régimen regulatorio europeo en protección de datos y su recepción en la Argentina

Nuestra regulación a la fecha, así como la amplia mayoría de las regulaciones latinoamericanas en materia de protección de datos personales, ha seguido la orientación y desarrollos históricos que se originaron en Europa y su modelo protectorio. En líneas generales, las legislaciones latinoamericanas se han centrado en la protección de los derechos a la intimidad y privacidad, así como en la acción de hábeas data, lo que se ha incluido expresamente en sus constituciones, así como en leyes especiales, tal como es el caso argentino (8).

La regulación europea en materia de protección de datos personales ha sido de avanzada en el resguardo de las garantías individuales. Encuentra su sustrato jurídico en la protección del derecho fundamental a la intimidad y privacidad que garantiza la Convención Europea de Derechos Humanos del año 1950 en su art. 8º.

La Unión Europea como región ha buscado garantizar principiológicamente la aplicación sistemática de este derecho desde su fundación en adelante. Para ello creó un marco institucional reforzado donde se plasmaron

normas centrales y uniformes exigibles a nivel regional, de las cuales derivarían las legislaciones nacionales europeas en concordancia con las normas superiores. Este marco institucional al que se hace referencia en la actualidad está compuesto por el Tratado de Lisboa del año 2007 y el Programa de Estocolmo y el Consejo Europeo de junio de 2014, donde se fijó entre los objetivos de la región la optimización en la protección de datos personales.

Por su parte, la Carta de los Derechos Fundamentales de la Unión Europea garantiza en particular en sus arts. 7º y 8º el derecho a la vida privada y la protección de los datos de carácter personal como derechos humanos autónomos y fundamentales.

En lo que respecta a la regulación central en protección de datos personales, el Convenio 108 de 1981 o Convenio de Estrasburgo fue el primer cuerpo sistematizado regional e internacional en el que se trató específicamente la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, sustentando en el derecho a la privacidad, del cual se derivaron las directivas y los reglamentos.

Los instrumentos legislativos regionales a nivel europeo en temáticas relativas a la protección de datos personales elaborados son los siguientes: la Directiva 2002/58/CE (9), modificada en 2009, sobre la privacidad y las comunicaciones electrónicas, la Directiva 2006/24/CE (10) sobre la conservación de datos (declarada inválida por el Tribunal de Justicia de la Unión Europea el 8 de abril de 2014 por infringir el derecho a la vida privada y la protección de datos), el Reglamento (CE) 45/2001 (11) sobre tratamiento de datos personales por instituciones y organismos comunitarios, la Decisión Marco del Consejo de 2008 (12) relativa a la protección de datos personales en relación a tareas de cooperación policial y judicial en materia penal.

El instrumento central, imitado por nuestra legislación, que se encontró vigente hasta el 25 de mayo de 2018, ha sido la Directiva 95/46/CE (13) (Reglamento general de protección de datos) relativa a la protección de datos, del 24 de octubre de 1995 (14).

Esta directiva se ocupaba de regular la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, centrada en el principio de información y consentimiento explícito del titular de los datos, así como la libre circulación de estos. A su vez, establecía las condiciones generales de licitud de tratamiento, al mismo tiempo que enunciaba y definía los derechos de sus titulares, así como la definición de autoridades en la materia que debían actuar a nivel local.

A modo de síntesis, la Directiva 95/46/CE sirvió de estándar uniformador para las legislaciones en protección de datos, no solo de la Unión Europea sino también de todo el mundo.

A más de una década de su vigencia, e impulsada en los últimos años, se gestó la reforma y derogación de la Directiva 95/46/CE por el Reglamento del Parlamento Europeo y del Consejo (UE) 2016/679 (15) y la Directiva (UE) 2016/680 (16), dirigida a reformular la legislación de la Unión, salvaguardar los derechos de protección ya asentados profundizando su tutela, al mismo tiempo que procuró otras finalidades, relativas a la circulación de datos y la satisfacción de necesidades de índole económica-empresarial.

La reforma de 2016 se dio como respuesta a los cambios que evidenció el acceso, la recolección, el procesamiento y uso, así como el intercambio de los datos en los últimos tiempos, escenario tecnológico muy diverso respecto de aquel en el que se gestó la Directiva 95/46/CE.

A partir de ello, se les otorgó a los países integrantes de la región un plazo de dos años para adecuarse al nuevo marco regulatorio. Así lo hicieron, modificando sus respectivas leyes especiales, los países que así lo requerían, o creando protocolos de aplicación o adecuación.

El 25 de mayo de 2018 entraron en vigor el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, junto con la Directiva (UE) 2016/680, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

La primera norma mencionada tiene por objetivo asegurar un marco de protección uniforme a nivel regional y de aplicación directa a los países miembros de la Unión, sin necesidad de adecuación legislativa local, dando un plazo generoso de dos años en cuanto a su entrada en vigencia y aplicabilidad, mientras que la segunda busca otorgar una normativa central y armónica en materia de cooperación transfronteriza en la región en la persecución delictiva y protección de datos que para ello se utilicen (17).

Entre sus contribuciones, se encuentran la profundización del sistema protectorio y los principios relativos al tratamiento de datos personales y al tratamiento de las categorías especiales de datos que define, la

modernización y ampliación de conceptos, así como la incorporación de otros, la conservación de los derechos reconocidos de los titulares de los datos, y la facilitación de tareas a las empresas, por su introducción en la aldea comercial regional.

Las novedades troncales que introduce giran en torno a la jerarquización de la importancia del consentimiento expreso del titular del dato, el que caracteriza como "... un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen...", el que debe ser demostrable por el responsable de tratamiento, la introducción del derecho al olvido y el derecho de portabilidad de datos, así como a la creación de la figura del Delegado de Protección de Datos, el que debe ser nombrado en cada organismo público —a excepción de algunos— con el fin de velar por el cumplimiento del Reglamento en aquellos operadores que traten volúmenes de datos a gran escala.

Nuestra similitud regulatoria con el modelo europeo de protección de datos se dio centralmente con el objetivo de facilitar la transferencia de datos desde Europa, actividad fundamental de la industria de tratamiento y requerimiento básico por su carácter transnacional.

Es así que la Argentina fue considerada en el año 2003, por la "Decisión de la Comisión del 30/06/2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina", como país adecuado para el tratamiento de datos personales conforme con el estándar europeo.

Claro está que, frente a la modificación del régimen europeo y tal como cualquier otro parámetro de certificación, al variar el marco regulatorio, dicha calificación indefectiblemente cae por cambiar las circunstancias que permitieron su afirmación.

Es así que, desde la entrada en vigor del nuevo régimen europeo, tanto nuestro país como los otros indicados como países adecuados para el tratamiento según sus estándares, debemos nuevamente adecuarnos para preservar dicha calificación.

También es necesario mencionar que el sector privado respondió de manera particular a la adecuación al nuevo Reglamento General europeo, uniformando su regulación, efectuando auditorías, tareas relativas al compliance normativo del nuevo reglamento, informes y evaluaciones, capacitaciones y aggiornamiento de procedimientos internos de tratamiento, en la medida de sus posibilidades y según su caso particular, de manera más o menos robusta.

Entre los fundamentos del Proyecto de Reforma de la Ley de Protección de Datos Personales enviado al Congreso de la Nación en septiembre de 2018, se citan, además de dotar a nuestro país de una regulación moderna y actualizada, los antecedentes del nuevo contexto internacional en la materia, en alusión a la reforma del régimen europeo.

Es por ello que entre los fundamentos expuestos señala: "... Cabe destacar que la República Argentina desde el año 2003 es considerada por la Unión Europea como un país con legislación adecuada para la protección de los datos personales (Comisión de las Comunidades Europeas - Decisión de la Comisión C [2003]1731 de fecha 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina). Sin perjuicio de esto, se advierte que esta situación puede cambiar con la adopción del Reglamento (UE) 2016/679, motivo por el cual se propone la presente reforma con la finalidad de mantener los estándares internacionales a los que nuestra legislación supo adaptarse, lo cual traerá consigo nuevas posibilidades de innovación e inversión en nuestro país...". A su vez, y como referencia para el contenido de la reforma proyectada y su texto, se expresó que se ha tenido en cuenta la regulación internacional citada, entre ellas la europea.

IV. El Proyecto de Reforma de la Ley de Protección de Datos Personales

El Proyecto de Reforma de la Ley de Protección de Datos Personales, presentado al Congreso de la Nación el 19 de septiembre de 2018, sigue aproximadamente la estructura que tenía la ley 25.326 en cuanto a la sucesión de su articulado y la progresividad de cómo se suceden las temáticas planteadas, a excepción, claro está, de los artículos y segmentos que introducen temáticas o figuras novedosas anteriormente no receptadas.

Claro está que, brevitatis causae, no es posible aquí efectuar un análisis granular con la extensión y profundidad que merece el articulado de dicho Proyecto, lo que podría demandar por lo bajo cientos de páginas; la intención del presente artículo es señalar su proyección, impactos y reflexiones que emanan de la nueva redacción propuesta, en sus aspectos más salientes, específicamente en lo atinente a sus definiciones, principios y derechos, por los grandes cambios que vendrán en la materia y que nos generarán, como operadores jurídicos, la impostergable tarea de trabajar con ellos, y evaluar sus posibles respuestas, desafíos y consecuencias desde el

plano legal y su repercusión en el ámbito de la protección de datos, así como en el de los derechos diversos que atañen a los titulares de los datos.

IV.1. Objeto

Conforme enuncia el art. 1º del Proyecto, "La presente Ley tiene por objeto la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares, de conformidad a lo establecido en el artículo 43, párrafo tercero, de la Constitución Nacional y los Tratados de Derechos Humanos en los que la República Argentina sea parte".

Dicha redacción concluye el debate doctrinario que surgía en torno al ámbito de aplicación, ya que en la ley 25.326 se enunciaba que "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes...", lo cual ocasionó desde lo técnico inmensa confusión. La protección integral del dato no puede verse limitada por la finalidad de la base de datos sobre la cual se encuentra asentada, por lo que resulta una clarificación positiva la simplificación del objeto que tutela la norma, en consonancia a cómo se enuncia el mismo en las normas observables de derecho comparado, que no han incurrido en ese error histórico.

IV.2. Definiciones

El art. 2º del Proyecto amplía el conjunto de definiciones de la norma, así como el nuevo Reglamento Europeo, el que también ensanchó este segmento introduciendo conceptos novedosos.

La ley 25.326 definía los conceptos de: datos personales, datos sensibles, archivo, registro, base o banco de datos, tratamiento de datos, responsable de archivo, registro, base o banco de datos, datos informatizados, titular de los datos, usuario de datos y disociación de datos.

El Proyecto, por su parte, define muchos más conceptos, como: autoridad de control, base de datos, datos personales, datos sensibles, disociación de datos, encargado del tratamiento, entidades crediticias, fuentes de acceso público irrestricto, fuentes de acceso público restricto, grupo económico, incidente de seguridad de datos personales, responsable de tratamiento, tercero, titular de los datos, transferencia internacional y tratamiento de datos.

Sin perjuicio de ello, lo cual resulta un innegable avance en consonancia con lo mencionado, existen ciertos puntos a destacar, los cuales resultan críticos en relación con el escenario actual en procesamiento de datos.

El primero de ellos es continuar definiendo al dato como sinónimo de información, error conceptual técnico en el que sigue incurriendo la regulación actual mayoritaria, puesto que la información son datos en relación, ambos conceptos son diversos en cuanto a funcionalidad y alcance. Un dato, en términos técnicos, es un registro, una representación formal de algo, un factor objetivo sobre algo determinado, mientras que la información es un conocimiento basado en datos procesados.

El segundo de ellos es definir que algo (una persona, por ejemplo) es indeterminable cuando "...para lograr su identificación, se requiera la aplicación de medidas o plazos desproporcionados o inviables", ya que ello no solo es un criterio subjetivo y circunstanciado al caso (p. ej., lo que resulta inviable para una organización que procesa datos de manera escasa resulta sobradamente viable para otra que se dedica a tareas de Big Data y minería de datos), sino que también se encuentra condicionado al momento científico.

Las técnicas de procesamiento de datos evolucionan a tal ritmo que aquello que hoy se concibe como imposible tal vez a poco de la entrada en vigor de la norma deje de serlo. Un clarísimo ejemplo de ello es la capacidad actual que existe de reversar, es decir, volver atrás los procesos de disociación de datos, por lo que todo el paradigma actual, que sostiene el procedimiento de disociación del dato como mecanismo seguro para seguir operando con datos una vez operado el cese de su finalidad de tratamiento, ya no es tal, sino que puede ser vulnerado.

El matiz abierto de la definición de dato sensible permite comprender o derivar razonablemente que las categorías de datos biométricos y datos genéticos, por su altísima sensibilidad, conforman parte de su tipología.

No obstante, resulta una oportunidad perdida continuar limitando la sensibilidad del dato a la capacidad de afectación de la esfera íntima del titular con potencialidad discriminatoria, puesto que la sensibilidad entendida en términos interdisciplinarios en procesamiento de datos no refiere únicamente a la discriminación, sino, más ampliamente, a la capacidad de afectar o dañar a su titular, lo cual nos hubiera situado de receptarlo en una legislación de punta y ejemplar en el tema.

Lo último referente en materia de definiciones es la relativa vaguedad conceptual, aunque se puede comprender que ello responde a alcanzar con esta norma un lenguaje más llano y cercano al lector. Del mismo

modo que enuncié mi opinión con respecto a la terminología utilizada por el unificado Código Civil y Comercial en su momento, la simpleza del lenguaje no puede afectar la precisión técnica que se requiere en la ley como herramienta del derecho, por lo que se debe intentar un balance, para que el hecho de utilizar un lenguaje menos complejo no implique vaguedad conceptual y discrecionalidad a costa de su simplificación, porque la seguridad jurídica no es un bien renunciable a cambio de ello.

IV.3. Principios relativos al tratamiento de datos

La ley 25.326 receptaba los principios de licitud, calidad de los datos, consentimiento, información, seguridad, confidencialidad, cesión y transferencia internacional, como aquellos relativos al tratamiento de categorías específicas de datos. Por su parte, en la reforma se proyecta la introducción de nuevos principios, así como la modificación de los parámetros de algunos de los enunciados.

Se plantea en el Proyecto de Reforma, al igual que el régimen europeo actual, el principio de extraterritorialidad en el art. 4º, cuyos supuestos enuncian en cuanto al ámbito de aplicación: "Las normas de la presente Ley serán de aplicación cuando: a. El responsable del tratamiento se encuentre establecido en el territorio nacional, aun cuando el tratamiento de datos tenga lugar fuera de dicho territorio; b. El responsable del tratamiento no se encuentre establecido en el territorio nacional, sino en un lugar en que se aplica la legislación nacional en virtud del derecho internacional; c. El tratamiento de datos de titulares que residan en la República Argentina sea realizado por un responsable del tratamiento que no se encuentre establecido en el territorio nacional, y las actividades de dicho tratamiento se encuentren relacionadas con la oferta de bienes o servicios a dichos titulares de los datos en la República Argentina, o con el seguimiento de sus actos, comportamientos o intereses; excepto cuando la ley del lugar donde se encuentra el responsable del tratamiento sea más favorable para la protección del titular de los datos".

El art. 5º del Proyecto enuncia los principios de lealtad, aplicable a los medios de tratamientos de los datos, los cuales no deben ser ni engañosos ni fraudulentos, y de transparencia, aunque no define qué implica esto último. Una interpretación posible de ello sería entender por transparencia el concepto actual que manejamos de transparencia informativa, la que debería versar no solo sobre qué datos se obtienen del titular y con qué finalidad se los procesa, sino también en informar a este sujeto de cómo se efectúa el tratamiento de los datos y en qué consiste su procesamiento.

Luego, en el art. 6º se encuentra receptado el principio de finalidad, que debe ser determinada, explícita y legítima, y el tratamiento de los datos deberá ser compatible con esta. No obstante, resulta una peligrosa afirmación aquello que se enuncia en su párrafo segundo, el que dice que "No se considerarán incompatibles con los fines iniciales tanto el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos, como tampoco el tratamiento de datos con fines que pudieron ser, de acuerdo al contexto, razonablemente presumidos por el titular de los datos", ya que aquello que razonablemente puede presumir un titular del dato se encuentra francamente limitado a aquello que puede imaginar desde su capacidad técnica, y el ensanchar la compatibilidad de finalidades expresas a aquellas que razonablemente se pueden presumir es algo no solo vago, sino que generará inseguridad jurídica.

En el art. 7º se enuncia el principio de minimización de datos, en el art. 8º el de exactitud, y en el 9º el principio de caducidad bajo el título "Plazo de conservación", principios cuya redacción resulta pertinente, clara y adecuada.

Por su parte, y tal como lo hiciera el nuevo régimen europeo, se introduce el principio de responsabilidad proactiva en el art. 10, lo cual resulta un gran avance, ya que pesa en cabeza del responsable de tratamiento el deber de demostrar a la autoridad de aplicación su cabal cumplimiento normativo y efectiva implementación de las medidas técnicas y organizativas que dispone la ley.

En lo que respecta al principio de licitud del tratamiento de datos, enunciado en el art. 11 del Proyecto, resulta necesario efectuar una detenida lectura del mismo completando su contenido, especialmente en sus supuestos más controvertidos, con las definiciones que la misma ley brinda, ya que cuando refiere a "consentimiento" debemos comprender que entiende por lícito todo aquello que la ley entiende por consentido, lo mismo respecto del tratamiento de datos de "fuentes de acceso público irrestricto", que en el art. 2º define como "Fuente de acceso público irrestricto: la que contiene información destinada a ser difundida al público, de libre acceso e intercambio por razones de interés general, accesible ya sea en forma gratuita o mediante una contraprestación", cuando ello podría generar incontables prácticas abusivas de perfilamiento conforme con las actuales y modernas técnicas de procesamiento de datos y la multiplicidad de bases de datos que revisten esta condición.

Por último, también es necesario detenerse en que se considerará lícito el tratamiento de datos conforme al inc. g), cuando "...sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del

tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente", lo cual podría dar lugar a abusos en el procesamiento por parte de los responsables de tratamiento, quienes unilateralmente, en principio, decidirían si su interés es legítimo y si, según su criterio industrial, este no cede frente al derecho humano del titular.

Una de las novedades más controversiales introducidas en los principios y que probablemente más nos distancian del nuevo régimen regulatorio europeo, es la redacción del art. 12 sobre consentimiento, en el que se prescribe que el tratamiento de datos requiere del consentimiento libre e informado, y que el mismo puede ser obtenido en forma expresa o tácita, receptando a su vez las excepciones que se listan en el art. 14 y la capacidad de revocarlo en cualquier momento en el art. 13.

Se define la admisibilidad del consentimiento tácito del siguiente modo: "El consentimiento tácito es admitido cuando surja de manera manifiesta del contexto del tratamiento de datos y la conducta del titular de los datos sea suficiente para demostrar la existencia de su autorización. Es admisible únicamente cuando los datos requeridos sean necesarios para la finalidad que motiva la recolección y se haya puesto a disposición del titular de los datos la información prevista en el artículo 15, sin que éste manifieste su oposición. El tratamiento de datos ulterior debe ser compatible con las finalidades manifiestas que surgen del contexto que originó la recolección. En ningún caso procede para el tratamiento de datos sensibles".

Sin perjuicio de que es posible considerar como antagónica la existencia de lo que se podría denominar sistemas de consentimiento, expreso y tácito, ya que el primero recepta excepciones, pero no admite el segundo, es a todas luces peligroso introducir la posibilidad de consentimiento tácito en relaciones jurídicas donde existe un sujeto vulnerable o débil jurídico.

Ni en el ámbito de los derechos del consumidor, ni en el ámbito de los derechos del paciente, se recepta en la actualidad la posibilidad de consentimiento tácito, por ser contradictorio con el paradigma protectorio vigente; la protección de datos no es ajena a ello, porque es otro de los tantos regímenes tuitivos de nuestro derecho.

Para enunciar un ejemplo muy gráfico de debilidad y potencia —relación experto a profano—, si una decisión sobre el cuerpo de un paciente fuera dependiente de lo que el médico unilateralmente decidiera sobre este bajo el precepto de que él presume la voluntad contextuada del paciente y entiende que surge de manera manifiesta del contexto y la conducta del paciente y la información que recibió, esto sería visto como un clarísimo ejemplo de paternalismo médico y como una aberrante conculcación al derecho de autodeterminación y autonomía de la voluntad del paciente y la disposición sobre su propio cuerpo, entre numerosísimos otros derechos humanos fundamentales que se verían vulnerados.

En materia de protección de datos personales, receptar la admisibilidad del consentimiento tácito es antagónico a la construcción del concepto de autodeterminación informativa del titular del dato, derecho humano fundamental sobre el cual se apoya la protección de sus datos personales.

Conforme con la definición que nos brinda el Dr. Eduardo Molina Quiroga, jurista nacional referente en materia de protección: "La protección de datos personales, autodeterminación informativa o libertad informática forma parte del núcleo de los derechos denominados de 'tercera generación'.

El derecho fundamental a la protección de los datos de carácter personal, como derecho de la llamada tercera generación, es uno de los exponentes del conflicto tecnología-Derecho, cuya razón de ser reside en dar al individuo la posibilidad efectiva de disponer y controlar los datos que le conciernen. Excede largamente el ámbito de la tutela a la intimidad o vida privada, aun cuando claramente la contiene"(18).

La autodeterminación informativa, derecho personalísimo de todo titular de gobernar los datos a él referidos, implica tres aristas a tener en cuenta: la autonomía de la voluntad del titular de los datos, el deber / derecho de información hacia el titular sobre los datos y acciones y condiciones de procesamiento que se efectúen sobre estos, y la información como sinónimo —inadecuadamente utilizado— del objeto jurídico protegido, los datos. En relación con esto último, se protege todo dato que procesado pueda transformarse en información.

El consentimiento tácito, conocido también como consentimiento fluido, no es otra cosa que aquello que requiere la industria de procesamiento de datos para agilizar su procesamiento, a costa del ejercicio del derecho de autodeterminación informativa de sus titulares.

El deber de información que pesa sobre el responsable de tratamiento, que se refleja en el derecho a la información del titular del dato, se expresa en el art. 15, en el que se enuncia a modo no taxativo la información que se le debe brindar al titular de los datos antes de su recolección.

Desde ya, hubiera sido un buen aporte incluir en el piso de información mínima a brindar la explicación al

titular del dato relativa a las técnicas de procesamiento a aplicar sobre sus datos, en qué consisten y cuáles son sus consecuencias.

El principio de seguridad de los datos en el art. 19 se encuentra redactado con claridad y evidencia un innegable avance muy útil en la materia, que guarda correlación con el art. 20 que le sigue, relativo a la notificación de incidentes de seguridad.

Prácticamente todas las legislaciones avanzadas en protección de datos personales enuncian el deber de notificar los incidentes en un plazo breve, como el que se expresa de 72 h, a la autoridad de aplicación de la norma o autoridad de control, así como el deber de comunicación a los titulares de los datos cuando del incidente de seguridad se pueda derivar la posibilidad de daño a su persona o bienes, por lo que resulta una excelente incorporación.

Las medidas de seguridad que se pueden adoptar deberán tomarse considerando al menos los siguientes factores que enuncia el art. 19 in fine: "a. El riesgo inherente por el tipo de dato personal; b. El carácter sensible de los datos personales tratados; c. El desarrollo tecnológico; d. Las posibles consecuencias de un incidente de seguridad para los titulares de los datos; e. Los incidentes de seguridad previos ocurridos en los sistemas de tratamiento".

Las medidas de seguridad para el tratamiento de datos personales fueron recientemente actualizadas por la resolución 47/2018 de la Agencia de Acceso a la Información Pública, que estableció las "Medidas de seguridad recomendadas para el tratamiento y conservación de los Datos Personales en medios informatizados", y derogó la disposición 11/2006, que reguló medidas posibles aplicables en la recolección de datos, control de acceso, control de cambios, respaldo y recuperación, gestión de vulnerabilidades, destrucción de la información, incidentes de seguridad y entornos de desarrollo.

La disposición 11/2006 anteriormente vigente regulaba las medidas de seguridad para el tratamiento y conservación de los datos personales, establecía la obligatoriedad para los "responsables registrados" de poseer un "Documento de Seguridad de Datos Personales" y cumplir con uno de los "tres [3] niveles de seguridad: básico, medio y crítico, conforme la naturaleza de la información tratada...", mientras que la actual resolución 47/2018 en su anexo I no indica qué medidas son aplicables conforme con el tipo de dato tratado, sino que libra todas ellas al arbitrio del responsable de tratamiento, recomendando su aplicación de modo referencial.

Por otra parte, la seguridad de los datos se complementa con lo normado en los siguientes artículos inspirados en el nuevo régimen europeo: el art. 37 del Proyecto "Medidas para el cumplimiento de la responsabilidad proactiva", el art. 38, "Protección de datos desde el diseño y por defecto", el art. 40, "Evaluación de impacto relativa a la protección de datos personales", el art. 41, "Contenido de la evaluación de impacto", y el art. 42, "Informe previo".

El deber de confidencialidad enunciado en el art. 21 y su ultraactividad en la etapa poscontractual se encuentra acabadamente redactado y no presenta confusiones o aristas conflictivas.

La cesión de datos, conforme con el art. 22 del Proyecto, enuncia claramente que "... el responsable del tratamiento a quien se ceden los datos personales queda sujeto a las mismas obligaciones legales y reglamentarias que el responsable cedente. Ambos responden por la observancia de aquéllas ante la autoridad de control y el titular de los datos de que se trate. En cualquier caso, podrán ser eximidos total o parcialmente de responsabilidad si demuestran que no se les puede imputar el hecho que ha producido el daño", por lo que el sistema de atribución de la responsabilidad establecido es objetivo y la responsabilidad es solidaria entre el responsable del tratamiento y el cesionario.

Régimen análogo se puede encontrar respecto del servicio de tratamiento de datos personales por medios tecnológicos tercerizados en el art. 26, aunque nuevamente en su redacción se repite como parámetro la razonabilidad del esfuerzo del responsable de tratamiento en elegir un proveedor que garantice el cumplimiento de la ley, lo cual es subjetivo e inadmisible en la temática, primando en ella factores objetivos atributivos de la responsabilidad (seguridad, información, etcétera).

Por último, en materia de transferencia internacional, en el art. 23, su licitud se encuentra condicionada al cumplimiento de al menos alguno de los siguientes supuestos: "a. Cuente 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; f. Sea necesaria en virtud de un contrato celebrado o por

celebrar en interés inequívoco del titular de los datos, por el responsable del tratamiento y un tercero; g. Sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; h. Sea necesaria para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; i. Sea necesaria para el mantenimiento o cumplimiento de una relación jurídica entre el responsable del tratamiento y el titular de los datos; j. Sea efectuada en los casos de colaboración judicial internacional; k. Sea requerida para concretar transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; 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; m. El responsable del tratamiento transferente y el destinatario adopten mecanismos de autorregulación vinculante, siempre y cuando éstos sean acordes a las disposiciones previstas en esta Ley; n. Se realice en el marco de cláusulas contractuales que contengan mecanismos de protección de los datos personales acordes con las disposiciones previstas en la presente Ley".

IV.4. Tratamiento de categorías específicas de datos y supuestos especiales de tratamiento

El Proyecto regula el tratamiento de categorías específicas de datos, a saber: datos sensibles en su art. 16, antecedentes penales y contravencionales en su art. 17 y datos de niñas/niños y adolescentes en su art. 18.

Por el art. 16, se prohíbe el tratamiento de datos sensibles, excepto cuando: "a. El titular de los datos haya dado su consentimiento expreso a dicho tratamiento, salvo en los casos en que por ley no sea requerido el otorgamiento de dicha autorización; b. Sea necesario para salvaguardar el interés vital del titular de los datos y éste se encuentre física o legalmente incapacitado para prestar el consentimiento y sus representantes legales no lo puedan realizar en tiempo oportuno; c. Sea efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud en el marco de un tratamiento médico específico de acuerdo a lo establecido por la Ley Nº 26.529 de Derechos del Paciente, Historia Clínica y Consentimiento Informado y sus modificatorias; d. Se realice en el marco de las actividades legítimas que realice una fundación, asociación o cualquier otro organismo sin fines de lucro, cuyo objeto principal sea una actividad política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan un contacto regular por razón de su objeto principal; e. Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; f. Tenga una finalidad histórica, estadística o científica. En estos dos [2] últimos casos, debe adoptarse un procedimiento de disociación de datos; g. Se refiera a datos personales que el interesado haya hecho manifiestamente públicos; h. Sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular de los datos en el ámbito del Derecho Laboral y de la Seguridad y Protección Social; i. Sea necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios; j. Se realice en el marco de asistencia humanitaria en casos de desastres naturales".

Puede llegar a resultar conflictivo en la práctica el inc. g), que refiere al tratamiento de datos sensibles cuando su titular los haya hecho manifiestamente públicos, puesto que el hacer público un dato no implica necesariamente que el titular de este haya brindado una autorización absoluta para su tratamiento irrestricto por cualquier sujeto. Esto puede devenir no solo en sorpresivo y abusivo para el mismo titular, sino engendrarle peligros tanto a su integridad psicofísica como económica, además de la afectación a sus derechos humanos personalísimos.

Por su parte, el art. 17 enuncia: "El tratamiento de datos relativos a antecedentes penales o contravencionales con el objeto de brindar informes a terceros sólo puede ser realizado por parte de las autoridades públicas competentes o bajo su supervisión.

"El empleador que conserve un certificado, documento o información de antecedentes penales o contravencionales de sus empleados no puede cederlo a terceros, salvo con el consentimiento expreso del titular de los datos".

El segundo párrafo presenta al menos una dudosa redacción. Resultaría contradictorio con el principio de caducidad y finalidad del dato que se conserven los antecedentes una vez cesada la relación laboral, y no resulta necesario aclarar que, si los conserva en vigencia de esta, cualquier cesión de dato del empleado que decida efectuar el empleador debe tener consentimiento expreso del empleado, sean estos u otros.

Por último, es destacable la incorporación de la categoría de sujetos hipervulnerables que constituyen en la aldea virtual los niños, niñas y adolescentes, y la protección de su interés superior conforme lo indica la regulación internacional de derechos humanos en la materia, la Convención sobre los Derechos del Niño.

El art. 18 reza: "En el tratamiento de datos personales de una niña, niño o adolescente, se debe privilegiar la

protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

"Es válido el consentimiento de una niña, niño o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos. En estos casos, el consentimiento es lícito si el menor de edad tiene como mínimo trece [13] años. Si la niña o niño es menor de trece [13] años, tal tratamiento únicamente se considera lícito si el consentimiento fue otorgado por el titular de la responsabilidad parental o tutela sobre la niña o niño, y sólo en la medida en que se dio o autorizó.

"El responsable del tratamiento debe realizar esfuerzos razonables para verificar, en tales casos, que el consentimiento haya sido otorgado por el titular de la responsabilidad parental o tutela sobre la niña, niño o adolescente, teniendo en cuenta sus posibilidades para hacerlo".

Es necesario mencionar que la regulación europea establece en el art. 8º, inc. 1º, del Reglamento que "...el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años", y nuestro proyecto optó por el piso mínimo que estableció ese marco, atendiendo al principio de capacidad progresiva.

En lo atinente a supuestos particulares de tratamiento, el Proyecto dedica un capítulo —el capítulo 6— a los "Servicios de Información Crediticia", en sus arts. 58 a 65 inclusive, y en el capítulo 7, "Supuestos Especiales", las "Bases de Datos Públicas" en el art. 66, el "Tratamiento de datos por organismos de seguridad e inteligencia" en el art. 67, y las "Bases destinadas a la publicidad" en el art. 68.

IV.5. Derechos de los titulares

El Proyecto enuncia los derechos de los titulares de los datos en su capítulo 3: derecho de acceso, derecho de rectificación, derecho de oposición, derecho de supresión, derechos en relación con las valoraciones personales automatizadas, derecho a la portabilidad de datos personales.

Asimismo, establece en el art. 35 la prohibición del abuso de derecho y las excepciones al ejercicio de los derechos enumerados en los arts. 27, 29, 30, 31, 32 y 33 en el art. 36, por su tratamiento en bases de datos públicas, las que deben ser fundadas en función de "la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros", o su información denegada cuando "... de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al titular de los datos".

El derecho de acceso, conforme con el art. 27, podrá ser ejercido por el titular de los datos "... previa acreditación de su identidad, tiene el derecho de solicitar y obtener el acceso a sus datos personales que sean objeto del tratamiento", y el contenido de la información que debe suministrarse al titular de forma clara y comprensible, según redacción del art. 28, 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", no podrá revelar datos de terceros y podrá suministrarse por medio escrito, electrónico u otros, en consonancia con el principio de equivalencia funcional y neutralidad tecnológica.

La rectificación de datos personales se encuentra reconocida como derecho en el art. 29 del Proyecto, frente a la inexactitud, falsedad, error, incompletitud o desactualización.

El derecho de oposición enunciado en el art. 30 procede cuando el titular del dato no ha prestado consentimiento, lo que se clarifica en la enunciación del artículo, el que dice: "El titular de los datos puede oponerse al tratamiento de sus datos, o de una finalidad específica de éste, cuando no haya prestado

consentimiento. El responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del titular de los datos".

Para interpretar el presente artículo es menester recordar la definición que brinda el sistema del Proyecto en materia de consentimiento, donde este se entiende prestado de manera expresa o tácita. A su vez, es necesario interpretar la prevalencia de los derechos del responsable de tratamiento de manera absolutamente restrictiva respecto de los titulares de los datos. Esa prevalencia debería únicamente proceder en aquellos supuestos que enuncia taxativamente el art. 36 citado previamente.

El art. 31 del Proyecto establece el derecho de supresión del siguiente modo: "El titular de los datos tiene derecho a solicitar la supresión de sus datos personales de las bases de datos del responsable del tratamiento cuando el tratamiento no tenga un fin público, a fin de que los datos ya no estén en su posesión y dejen de ser tratados por este último.

"La supresión procede cuando: a. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados; b. El titular de los datos revoque el consentimiento en que se basa el tratamiento de datos y éste no se ampare en otro fundamento jurídico; c. El titular de los datos haya ejercido su derecho de oposición conforme al artículo 30, y no prevalezcan otros motivos legítimos para el tratamiento de sus datos; d. Los datos personales hayan sido tratados ilícitamente; e. Los datos personales deban suprimirse para el cumplimiento de una obligación legal.

"La supresión no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, prevalezcan razones de interés público para el tratamiento de datos cuestionado, o los datos personales deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las contractuales entre el responsable o encargado del tratamiento y el titular de los datos.

"La supresión tampoco procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información".

En los fundamentos del Proyecto se enuncia puntualmente respecto del derecho de supresión que "... Este último derecho engloba lo que en la actualidad se conoce como 'derecho al olvido', denominación usualmente utilizada pero que ha traído muchas discusiones teóricas y críticas sobre su aplicación en la práctica, dado que una deficiente implementación podría devenir en violaciones a otros derechos fundamentales, como la libertad de expresión o el acceso a la información. De allí que en la propuesta que se somete a consideración, si bien se reconoce este derecho, se ha aclarado especialmente que el derecho de supresión no procede cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información".

Por "derecho al olvido" / "right to oblivion" / "droit à l'oubli", se entiende aquel derecho que posee el individuo a ser olvidado, a que la información que se refiera a este sea borrada —por su contenido y transcurso del tiempo— (19).

El derecho al olvido digital en nuestro sistema, en miras a la protección de la libertad de expresión y la prohibición de la censura previa, recepta mayores limitaciones que en el marco regulatorio europeo donde se lo reconoce en el art. 17 del Reglamento vigente.

En nuestro sistema no procede la remoción de contenidos por particulares, ya que la supresión de datos irrestricta y desregulada, sin control judicial suficiente, redunda en una causación de perjuicios a derechos e intereses legítimos de terceros individuales y colectivos, humanos, sociales y culturales. Es por ello que en nuestro sistema la decisión de supresión o remoción debe provenir de una autoridad judicial y no de los particulares, sean estos individuos o empresas.

Por último y para concluir, también reconoce el Proyecto el derecho a la portabilidad de datos personales, derecho reconocido a su vez por el Reglamento Europeo en su art. 20.

El art. 33 del Proyecto dice lo siguiente: "Si se brindan servicios en forma electrónica que incluyan el tratamiento de datos personales, el titular de los datos tiene derecho a obtener del responsable del tratamiento una copia de los datos personales objeto de tratamiento en un formato estructurado y comúnmente utilizado que le permita su ulterior utilización. El titular de los datos puede solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

"Este derecho no procederá cuando: a. Su ejercicio imponga una carga financiera o técnica excesiva o irrazonable sobre el responsable o encargado del tratamiento; b. Vulnere la privacidad de otro titular de los datos; c. Vulnere las obligaciones legales del responsable o encargado del tratamiento; d. Impida que el responsable del tratamiento proteja sus derechos, su seguridad o sus bienes, o los derechos, seguridad y bienes

del encargado del tratamiento, o del titular de los datos o de un tercero".

Cabe destacar que el derecho a la portabilidad de los datos personales debe garantizarse en las condiciones que exige la norma y bajo los principios de tratamiento que esta misma establece, tal como lo indica el artículo citado in fine.

Por otra parte, no resulta razonable el inc. a), en el que se establece que la posibilidad del ejercicio de este derecho dependerá de lo excesivo o no, o razonable o no, que resulte para el responsable de tratamiento garantizarlo, puesto que, si este ha decidido profesionalmente desarrollar su actividad y ofrecer el servicio de tratamiento de datos personales, no puede bajo estos pretextos de manera legítima sustraerse de sus deberes inherentes de cumplimiento.

Resulta, a estos mismos efectos, mucho más razonable al caso que el responsable de tratamiento se abstenga de tratar los datos de los titulares y se abstenga de insertarse en una actividad económica y técnica específica determinada, que es el procesamiento de datos, hasta tanto no sea capaz de garantizar los derechos de los titulares de los datos, la protección de sus datos personales y el tratamiento de los datos bajo el marco de los principios de tratamiento que exige la norma.

V. Conclusiones y reflexiones finales

Como se ha podido ver en este primer acercamiento a la regulación que propone el Proyecto de Reforma de la Ley de Protección de Datos Personales, presentado en septiembre de 2018 en el Congreso de la Nación, este importa un escenario novedoso en materia de conceptos, principios, derechos y obligaciones, así como deberes y figuras no tratadas específicamente en este artículo, tales como la del Delegado de Protección.

La redacción del Proyecto formula una propuesta innovadora, no solo respecto de la regulación previa de la ley 25.326, sino también respecto del marco regulatorio europeo que entró en vigencia el 25 de mayo de 2018, por lo que resta tanto su debate parlamentario como futura posible aplicación, para verificar en la práctica sus aciertos y desaciertos y la materialización de las reflexiones aquí planteadas.

El futuro en protección de datos personales es prometedor y nos plantea y enfrenta con desafíos inconmensurables desde lo técnico y lo legal, y es nuestra responsabilidad como profesionales del derecho velar por el avance y la garantía de los derechos humanos y fundamentales que se encuentran en juego, así como por su no regresividad.

Asimismo, no debemos perder en vista que el examen de textos normativos, como el que aquí se realiza, tiene por objeto la tutela de un sujeto vulnerable, el titular del dato, que se encuentra en condiciones desiguales frente a su contraparte, el responsable de tratamiento. Su desigualdad se funda en los mismos extremos que los que comparte con otro débil jurídico, el usuario o consumidor, por su debilidad económica, estructural e informativa.

Es por ello que resulta necesario que la redacción que tome esta norma fundamental y especial de protección de datos personales abrace esta circunstancia y priorice el cumplimiento del derecho humano fundamental y personalísimo a la autodeterminación informativa del titular, por sobre el desarrollo avasallante que plantea la actividad industrial del procesamiento de datos.

El camino recorrido para alcanzar este momento de transición regulatoria ha sido extenso y aún resta mucho por delante, por lo que seguirá requiriendo de la participación y el compromiso profesional de todos, como así también el aporte y la apertura interdisciplinar a la realidad del objeto que regula, puesto que muchos errores que se suelen cometer en materia regulatoria ocurren por la ausencia del aporte técnico pertinente y la comprensión genuina y acabada de las consecuencias del hecho técnico regulado.

Por todo lo cual se espera que así sea y que nuestro futuro régimen de protección de datos en la Argentina nos ofrezca un entorno tuitivo robusto y sólido, que enaltezca la garantía y el ejercicio de los derechos humanos fundamentales en juego.

(*) Consultora, asesora y representante legal especializada para Argentina, LATAM y Caribe en Derecho Informático, Data Privacy e Infosecurity, entre otras temáticas. Directora de Faliero Attorneys At Law. Doctoranda y especialista en Derecho Informático y abogada en Derecho Empresarial y Privado (F. Derecho UBA). Profesora (F. Derecho UBA, F. Ingeniería UNDEF, F. Derecho USAL, F. Derecho y F. Ingeniería UP, ADACSI-ISACA Bs. As. Chapter), investigadora adscripta Inst. Gioja, UBACyT, DeCyT y PII.

(1) Ley 25.326, art. 1º: "(Objeto). La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo

establecido en el artículo 43, párrafo tercero de la Constitución Nacional."Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal."En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas".

(2) Puccinelli, Oscar R., "Argentina frente a los requerimientos de la comunidad europea en materia de tratamiento de datos personales: es tiempo de cambios", MJ-DOC-3184-AR | MJD3184, 6/7/2007.

(3) Decreto 899/2017, Acceso a la información pública. Modificación por decretos 1558/2001, 357/2002 y 1172/2003. Ciudad de Buenos Aires, 3/11/2017. Art. 2º: "Toda referencia normativa a la Dirección Nacional de Protección de Datos Personales, su competencia o sus autoridades, se considerará referida a la Agencia de Acceso a la Información Pública".

(4) Disponible en: https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf.

(5) Primera versión del Anteproyecto de Reforma de la Ley de Protección de Datos Personales. Disponible en: https://www.argentina.gob.ar/sites/default/files/anteproyecto_de_ley_de_proteccion_de_los_datos_personales.pdf.

(6) Segunda versión del Anteproyecto de Reforma de la Ley de Protección de Datos Personales. Disponible en: https://www.argentina.gob.ar/sites/default/files/anteproyecto_reforma_ley_proteccion_de_los_datos_personales_nueva_version.pd

(7) Proyecto de ley: INLEG-2018-46290265-APN-PTE, Ciudad de Buenos Aires, miércoles 19 de septiembre de 2018, ref.: EX-2017-01309839-APN-DGDYD#SLYT - Proyecto de Ley Datos Personales.

(8) Puccinelli, Oscar R., "Argentina frente a los requerimientos...", cit.

(9) Disponible en: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_es.pdf (4/3/2017).

(10) Disponible en: https://www.boe.es/doue/2006/ 105/L00054-00063.pdf (4/3/2017).

(11) Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/application/286_es.pdf (4/3/2017).

(12) UE. Decisión Marco 2008/977/JAI del Consejo, del 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32008F0977&from=ES (4/3/2017).

(13) Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML (4/3/2017).

(14) Martínez, Matilde S., "Nueva propuesta del Parlamento Europeo y del Consejo relativa a la protección de datos personales. Protección de datos en el entorno digital. La realidad argentina", MJ-DOC-6339-ARMJD6339, 2/7/2013.

(15) Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES (4/3/2017).

(16) Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES (4/3/2017).

(17) Actiance, "GDPR Compliance and Its Impact on Security and Data Protection Programs", Osterman Research White Paper, January 2017. Disponible en: https://www.mimecast.com/globalassets/documents/whitepapers/gdpr_compliance-_-impact_on_security_and_data_protection-pro (21/12/2017).

(18) Molina Quiroga, Eduardo, "Aplicación del principio de calidad en el tratamiento de datos personales", Sup. Const. del 18/2/2014, p. 57, LL 2014-A-341.

(19) Véase Fleischer, Peter, "The right to be forgotten, or how to edit your history", en HYPERLINK "http://peterfleischer.blogspot.com.ar/" Peter Fleischer: Privacy...? Blog, 29/1/2012, http://peterfleischer.blogspot.com.ar/2012/01/right-to-be-1/forgotten-or-how-to-edit.html; Kozinski, Alex, "The Dead Past", SLR Online. Perspectives. The Privacy Paradox, 64 Stanford Law Review Online 117, 12/4/2012, HYPERLINK "http://www.stanfordlawreview.org/online/privacy-paradox/dead-past"http://www.stanfordlawreview.org/online/privacy-paradox/d