por los Derechos Civiles

Volumen I

Análisis inicial del proyecto de ley de protección de datos personales de Argentina

Octubre 2018

Análisis inicial del proyecto de ley de protección de datos personales de Argentina*

El 19 de septiembre de 2018, el Poder Ejecutivo Nacional envió el proyecto de ley de protección de datos personales al Congreso de la Nación[1]. La iniciativa fue dirigida al Senado, que actuará como Cámara de origen y será considerada por las Comisiones de Asuntos Constitucionales y de Derechos y Garantías. De esta manera, comienza legislativamente el proceso para sancionar una normativa que viene generando expectativa en el sector público, diversas compañías privadas, el Poder Judicial, la academia y las organizaciones de defensa de los derechos humanos, entre otros ámbitos.

A continuación, la Asociación por los Derechos Civiles (ADC) presenta su análisis inicial del proyecto. El documento está basado en anteriores posicionamientos que tuvo la organización en instancias previas de discusión de la presente iniciativa[2] y, también, en nuevas conclusiones surgidas de las diferencias de redacción que existen en la propuesta finalmente enviada al Congreso.

La propuesta responde a la necesidad de actualizar el marco legal vigente a fin de ponerlo a tono con los desafíos del desarrollo y la masificación de las tecnologías digitales. En ese sentido, la adopción de figuras como la del delegado de protección de datos, la de evaluación de impacto o la de "privacidad por diseño y por defecto" constituyen herramientas que pueden contribuir a incrementar la función preventiva del derecho de la protección de datos, evitando el daño antes de que se produzca.

Sin embargo, existen múltiples aspectos que pueden ser mejorados para poder cumplir de una mejor manera los propios objetivos que el proyecto se propuso lograr. A continuación, enumeraremos algunos de ellos.

1. La protección de datos personales como medio para compensar situaciones de asimetría. El principio "*in dubio pro* titular del dato": Como comentario inicial, se debe resaltar

*El presente documento fue escrito por **Eduardo Ferreyra,** abogado y analista de políticas públicas del Área Digital de la Asociación por los Derechos Civiles (ADC). https://adcdigital.org.ar | https://adc.org.ar Este documento se encuentra bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

[1] El proyecto puede ser consultado en https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf (último acceso: 11/10/2018)

[2] Ver Asociación por los Derechos Civiles, Comentarios al anteproyecto de ley de protección de datos personales, Buenos Aires, 2017, disponible en https://adcdigital.org.ar/wp-content/uploads/2017/03/Comentarios_leyPDP.pdf (último acceso: 11/10/2018)

una característica fundamental de la relación entre el titular y el responsable (y/o encargado) de los datos: la asimetría de poder y conocimiento.

Es frecuente que los sujetos encargados de utilizar datos personales sean el Estado y las empresas o los grupos económicos que tratan grandes volúmenes de datos personales. Para llevar a cabo esta tarea, emplean técnicas y tecnologías que, generalmente, se encuentran a una distancia abismal del entendimiento del sujeto titular de los datos.

Por otro lado, la facilidad para tratar datos personales los ha vuelto un activo central para las operaciones de negocios y para una administración de gobierno más efectiva. Así, el manejo de datos se ha vuelto una forma de adquirir poder económico y control político por parte de empresas y gobiernos. Frente a esta situación, los individuos se ubican en un estado de vulnerabilidad producto de una desigualdad estructural de posiciones.

Esta distribución asimétrica de poder y saber debe ser el enfoque que nos guíe al momento de analizar las disposiciones de toda legislación que se proponga regular los datos personales.

Con esta pauta, debemos mencionar un rasgo del proyecto que puede perjudicar la protección de los datos de las personas: la amplia utilización de conceptos jurídicos indeterminados. En efecto, en el texto encontramos numerosos términos de vago significado, que pueden dar lugar a interpretaciones perjudiciales a los derechos de los titulares de los datos. Para mencionar solo algunos: "incompatibles" (art. 6), "expectativas razonables" (art. 12), "esfuerzo razonable" (art. 18 y 26) o "interés legítimo" (art. 11.g). Estos conceptos podrían provocar diversos problemas. Por ejemplo, el art. 12 sostiene que la forma del consentimiento –expreso o tácito– dependerá de –entre otros factores– las "expectativas razonables" del titular del dato. Si entendemos por tal aquellas que efectivamente tienen las personas, no es desatinado pensar que las mismas sean muy bajas, debido a la falta de conciencia y conocimiento acerca de la protección de datos personales que existe hoy en nuestra población. En consecuencia, los responsables estarían autorizados para conseguir el consentimiento tácito cuando lo más adecuado –en virtud de las razones mencionadas– tendría que ser el consentimiento expreso.

En consecuencia, si bien es difícil no recurrir a conceptos generales cuando se trata de redactar una norma que apunta a regular una pluralidad de casos a suceder en el futuro, no es menos cierto que términos amplios pueden ocasionar riesgos para los derechos de las personas, debido a la posibilidad de una mala interpretación de los mismos. Por lo tanto, consideramos necesario incluir en el proyecto ciertas pautas que restrinjan la interpretación de un concepto indeterminado o una excepción a un derecho.

En el sentido anterior, debería establecer expresamente el principio "*in dubio pro* titular del dato" como fórmula interpretativa que permita resolver aquellos casos en los cuales existan dudas sobre el alcance de un concepto o una excepción. De esta manera, se compensa la generalidad de los términos con una directiva clara ¬–en favor del titular del dato– a los órganos aplicadores de la ley.

2. Consentimiento: El proyecto admite que el consentimiento pueda ser otorgado de manera tácita. Así, se diferencia de la actual ley, que solo permite el consentimiento "expreso". Si bien entendemos que la introducción de esta figura responde a un intento de promover el libre flujo de datos que el desarrollo de una economía digital requiere, no debemos olvidar que la protección de datos personales asumió como meta principal el resguardo del individuo. Es por ello que las disposiciones deben ser redactadas con sumo cuidado, a fin de evitar abusos por parte del sector más poderoso en la relación jurídica. En ese sentido, queremos llamar la atención sobre el criterio que el anteproyecto utiliza para delimitar cuándo el consentimiento debe ser dado de manera expresa o tácita (art.12).

Al decir que la forma dependerá de "las circunstancias, el tipo de dato personal y las expectativas razonables del titular de datos", la disposición incumple con su función de establecer una pauta clara que nos permita determinar con anticipación cuáles son los casos abarcados por una y otra categoría. De esta forma, es de prever que existirán interpretaciones en conflicto por parte del titular del dato y del responsable (o encargado), lo que puede dar lugar no solo a un aumento de la litigiosidad, sino también de desprotección del titular, que en muchos casos puede no tener cabal noción del consentimiento que –tácitamente– estaría prestando.

Por otro lado, la vaguedad de los conceptos resulta una invitación a que los responsables (o encargados) favorezcan un tratamiento basado en el consentimiento tácito, dejando al consentimiento expreso para casos excepcionales.

Finalmente, apelar a las expectativas razonables del titular del dato puede resultar perjudicial en el siguiente sentido: debido a que su situación de debilidad suele traducirse en una ausencia de conocimiento acerca de los derechos que le corresponden y de los límites que deben existir al momento de tratar sus datos, no es de esperar que sus expectativas sean demasiado altas, con lo que este requisito puede volverse una carta libre para un tratamiento indiscriminado de sus datos.

Asimismo, esta situación de incertidumbre se repite al momento de calificar las condiciones para que surja el consentimiento tácito. Establecer que el consentimiento surgirá de "manera manifiesta del contexto de tratamiento de datos" o que la "conducta del titular de los datos" será "suficiente para demostrar la existencia de su autorización" puede volverse una tarea absolutamente discrecional sin pautas o guías que orienten su interpretación.

En consecuencia, consideramos que una adecuada regulación debe seguir considerando al consentimiento expreso como la regla general del sistema, ya que es el medio más eficaz para determinar de manera inequívoca que el titular del dato dio su acuerdo para que sus datos sean tratados.

Por otro lado, debería establecerse que, en caso de duda, se entenderá que el consentimiento es requerido de manera expresa. Asimismo, debería mantenerse el requisito –presente en nuestra actual ley– de que el consentimiento también debe ser libre e informado, sin perjuicio de adoptar definiciones más modernas.

Por último, debería establecerse en forma excepcional y detallada los casos en los que puede aplicarse el consentimiento tácito. A fin de prever futuras situaciones que justifiquen la conveniencia de requerir un consentimiento tácito, podría facultarse a la autoridad independiente de control a extender –de manera fundada– dichas excepciones, cuando sea estrictamente necesario.

3. Fuentes de acceso público irrestricto: El proyecto sostiene que, para realizar tratamiento de datos obtenidos de fuentes de acceso irrestricto, no se requerirá el consentimiento del titular del dato (art. 11.b). A su vez, el art. 2 establece que fuente de acceso público irrestricto es 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".

Tal característica parece, en principio, justificar el no requerir consentimiento, ya que se trataría de información que está al alcance de todos. Sin embargo, dicho pensamiento omite el impacto que las tecnologías de recopilación y almacenamiento de información tienen para el ejercicio de actividades de perfilamiento y vigilancia. Con el actual desarrollo tecnológico, la recolección de información que las personas dejan a través de Internet y otros entornos digitales se ha convertido en una herramienta que permite la elaboración de perfiles y el ejercicio de actividades de vigilancia sobre los individuos. Esto ha llevado a que la investigación de fuentes abiertas sea uno de los principales métodos utilizados por las fuerzas de seguridad en Argentina.

Estas actividades pueden conllevar un serio riesgo para los derechos y las libertades de las personas. De este modo, el hecho de que dichas prácticas se realicen en base a datos surgidos de fuentes consideradas de "acceso público irrestricto" no debe ser un justificativo para otorgar una discrecionalidad absoluta a los responsables o encargados de un tratamiento de esa naturaleza. En consecuencia, consideramos que, si el tratamiento y la cesión de datos basado en fuentes de este tipo tiene por objeto la realización de actividades de perfilamiento o *profiling*, vigilancia u otra actividad sensible, debería contar con el consentimiento del titular de datos, sin perjuicio del cumplimiento de las demás garantías que la ley establece.

4. Metadatos: Resulta conveniente incluir una disposición que expresamente extienda la protección de la ley a los metadatos, es decir, aquella información que se refiere al origen, destino, duración, fecha, hora y ubicación de las comunicaciones. El motivo es la importancia que revisten los mismos, en tanto permiten revelar tanto o más acerca de nosotros que el propio contenido de las comunicaciones. Así, a través de ellos se pueden establecer patrones de comportamientos, hábitos o relaciones, por lo que actualmente constituyen una de las formas más eficaces de violar la privacidad de los individuos. Si bien existe consenso en que los metadatos son datos personales en tanto permiten la identificación de una persona, no sería irrelevante su determinación expresa, a fin de ahuyentar eventuales interpretaciones restrictivas.

5. Tratamiento de datos con fines de seguridad pública o defensa nacional: Por la sensibilidad del tema, debería sancionarse una ley específica que regule de modo integral el tratamiento de datos

por parte de las fuerzas de seguridad, al estilo de la Directiva 680/16 de la Unión Europea[3]. Mientras tanto, algunas medidas que pueden incorporarse al proyecto de ley para salvaguardar los derechos de las personas incluyen: a) el establecimiento de plazos para la supresión de los datos personales o para su revisión periódica, a fin de evaluar la pertinencia de su almacenamiento; b) la distinción entre datos personales recabados en base a hechos, de aquellos que puedan derivarse de apreciaciones personales, opiniones, juicios de valor propios de los agentes que realizan las tareas de seguridad o de defensa; c) el aumento de los requisitos para el tratamiento de datos, como exigir la presencia de un "peligro real" para la seguridad pública.

6. El manejo estatal de los datos personales: Una de las principales falencias de nuestra actual legislación es la amplia discrecionalidad que otorga al Estado para tratar los datos de las personas. En particular, el requisito del consentimiento para la recolección de datos no es requerido cuando se trata de "funciones propias de los poderes del Estado" (art. 5 inc. 2 b, ley 25.326) ni tampoco se lo exige para la cesión de datos "entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias" (art.11, ley 25.326)[4]. Esta facultad ha comenzado a ser restringida por la jurisprudencia debido a los problemas que planteaba desde el punto de vista constitucional, en especial, la afectación que se produce al derecho a la privacidad.

Así, en julio de este año, la Cámara en lo Contencioso y Administrativo Federal declaró en el fallo "Torres Abad" (2018)[5] que no requerir consentimiento para recolectar datos que serán utilizados en funciones propias del Estado equivale a una liberación en blanco que resulta excesiva y es por eso que debe haber una restricción. Este límite –según se desprende del referido fallo– debe ser que únicamente pueden recabarse y ceder datos sin consentimiento cuando se trate de datos recopilados con fines de defensa nacional, seguridad pública o represión de delitos. Para todo lo demás, habrá que obtener la autorización del titular del dato o encuadrar la situación en otra excepción de la ley. Sin dejar de señalar los potenciales peligros que puedan surgir de una habilitación amplia para tratar datos personales con fines de seguridad[6], la sentencia constituye un esfuerzo por empezar a establecer límites al manejo estatal.

En este sentido, el proyecto no se ajusta a lo sostenido por la más moderna jurisprudencia. En

[3] 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 puede consultarse en https://publications.europa.eu/es/publication-detail/-/publication/182703d1-11bd-11e6-ba9a-01aa75ed71a1/language-es (último acceso: 11/10/2018)

[4] Sin perjuicio de otros supuestos de carácter general que también pueden aplicarse a la actividad estatal, como los casos en los que se trata de "listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio" (art. 5 inc. 2 c).

[5] El fallo puede descargarse en PDF en (descarga directa): https://bit.ly/2NpTC61 (último acceso: 11/10/2018)

[6] Sobre la necesidad de reforzar los límites en el tratamiento de datos personales para fines de seguridad en el caso de datos biométricos ver, Asociación por los Derechos Civiles, Desafíos de la biometría para la protección de los datos personales, 2017, disponible en https://adcdigital.org.ar/wp-content/uploads/2017/06/ADC-Biometria-y-proteccion-de-datos-personales.pdf (último acceso: 16/10/2018).

efecto, el art. 11 inc. c exime al Estado de conseguir el consentimiento cuando "el tratamiento de datos se realice en ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias". De esta manera, se omite consagrar el estándar fijado por "Torres Abad" y así, el sector público continúa gozando de una gran discrecionalidad para utilizar los datos de las personas.

Para reforzar esta consideración, debemos mencionar dos disposiciones adicionales del proyecto. La primera es el art. 14, que agrega al listado actual previsto en la ley 25.326 el correo electrónico como dato que no necesita del consentimiento del titular para ser tratado. Esta inclusión tiene por consecuencia eliminar lo decidido en "Torres Abad", respecto a que es necesario el consentimiento del titular para que el correo electrónico –y el número telefónico– puedan ser tratados y cedidos.

La segunda es que el proyecto establece que la "satisfacción de un interés legítimo" será considerada una condición válida para la licitud de un tratamiento de datos por parte de las autoridades (art. 11 inc. g). Esto marca una diferencia con el anteproyecto elaborado por la autoridad de protección de datos, en el cual se contemplaba expresamente que dicha condición no aplicaba al sector público (art. 11 *in fine* anteproyecto versión final). De esta manera, y tal como está formulado el proyecto de ley, el Estado gozará de amplia discrecionalidad para tratar los datos de las ciudadanas y los ciudadanos que posea en sus bases, en tanto la noción de "interés legítimo" adolece de la suficiente vaguedad como para justificar diversos tipos de utilización de información personal.

En definitiva, el proyecto sigue tratando con excesiva deferencia los diversos manejos que el Estado puede realizar con nuestra información personal. Esto resulta preocupante, ya que se corre el riesgo de perder la oportunidad de establecer límites más claros y estrictos a un sujeto como el Estado, que lleva a cabo diariamente operaciones de tratamiento de datos masivas y de gran impacto en las personas.

7. Legitimación para reclamar por violaciones a la protección de datos: En el art. 81 el proyecto elimina lo dispuesto en el anteproyecto[7] respecto a ampliar la legitimación activa en caso de violaciones generalizadas. Así, el Defensor del Pueblo, las asociaciones sectoriales y el Ministerio Público, ya no están facultados para interponer la acción de *habeas data* en caso de una afectación colectiva, como sucedía en el anteproyecto (art. 79 anteproyecto versión final). Esta disposición había sido incluida luego de un comentario de la ADC en el sentido aludido y respondía a la realidad de que numerosas vulneraciones a la protección de datos tienen lugar a través de violaciones masivas que perjudican a una pluralidad de personas, mediante un mismo acto. De esta forma, el proyecto no reconoce debidamente las consecuencias procesales de que un derecho revista carácter colectivo, despojando a las personas de una herramienta clave para la defensa de sus intereses.

[7] El anteproyecto fue elaborado por la autoridad de protección de datos de Argentina luego de haber analizado aportes y comentarios a una primera versión del mismo a través de la plataforma Justicia 2020. El texto sirvió como base para el proyecto final del Poder Ejecutivo y puede consultarse en https://bit.ly/2PQeUrv (último acceso: 11/10/2018)

8. Intervención humana en decisiones automatizadas: Por último, la propuesta suprimió el derecho de toda persona a exigir, en casos de valoraciones automatizadas, la intervención humana en la toma de decisiones, así como a expresar su punto de vista o impugnar la decisión. Estos derechos estaban consagrados en el anteproyecto (art. 32 anteproyecto, versión final), como estándar mínimo a cumplir por parte del responsable del tratamiento de datos, y resultaban un límite sustancial para prevenir situaciones de injusticia causadas por el uso de algoritmos u otros métodos automatizados de decisión. Al quitarse esta disposición, queda exclusivamente a criterio del responsable del tratamiento de los datos mediante decisiones automatizadas, el decidir cuáles son las medidas adecuadas para salvaguardar los derechos del titular de los datos. De este modo, el Estado se abstiene de imponer obligaciones más intensas a aquellos sectores que pueden hacer un uso continuo de estas herramientas y así, poner en riesgo los derechos de las personas. En consecuencia, se produce una reducción de las garantías otorgadas.

9. Transferencias internacionales: El proyecto de ley establece diversas causales para autorizar la cesión de datos de personas residentes en Argentina hacia otros países. Además del consentimiento expreso del titular o de que el país ¬–u órgano internacional– cuente con un nivel adecuado de protección de datos, existen otros supuestos que merecen ser considerados con atención. La razón es que, en estos otros casos, información privada de las personas puede ser enviada sin su autorización a naciones que habilitan un manejo más discrecional de la misma. En particular, merecen nuestra atención los siguientes casos:

a) Cuando Argentina sea parte de un tratado: los datos constituyen la materia prima sobre la cual las empresas del sector tecnológico basan sus modelos de negocios y obtienen sus ganancias. De esta manera, las presiones por flexibilizar el flujo de datos a través de una liberalización del comercio electrónico han llegado a la agenda de discusión de los gobiernos en el marco de la Organización Mundial del Comercio (OMC). Intentos para conseguir un mandato que inicie conversaciones para negociar un tratado sobre comercio electrónico vienen llevándose a cabo continuamente[8]. En su defecto, la celebración de tratados bilaterales y multilaterales está siendo propuesta por diferentes naciones. En el caso de que este –o cualquier otro acuerdo que se alcance en otro foro o de manera bilateral o multilateral– se concrete y Argentina sea parte, tal suceso serviría como justificación para enviar información privada de argentinos a naciones que no cuentan con niveles de protección adecuados. De este modo se corre el riesgo de buscar la maximización de la renta empresarial a costa de una baja en el resguardo de los derechos de las personas.

b) Cesión a una sociedad del mismo grupo económico del responsable del tratamiento: La transferencia entre dos empresas del mismo grupo económico es otro supuesto que permite evadir la necesidad de conseguir el consentimiento del titular del dato o de exigir que el país receptor cuente

[8] Cfr. Ávila, Renata y Kilic, Burcu, Cuando lo que se negocia es nuestra privacidad: la Ministerial de la OMC en Buenos Aires, 2017, disponible en https://www.opendemocracy.net/democraciaabierta/burcu-kilic-renata-avila/la-omc-en-buenos-aires-o-c-mo-los-gigantes-digitales-comp (último acceso: 11/10/2018)

con un nivel de protección adecuado. Esta situación también debe ser examinada con cuidado porque hoy operan en el país varias empresas de naciones que, según nuestra legislación, no cuentan con dicho nivel[9]. Pensemos en el caso de sociedades de EE. UU. o de algunos países latinoamericanos (con excepción de Uruguay) cuyas normas en muchos casos otorgan menos protección que la brindada por la ley nacional. Bajo esta condición, tal situación no sería impedimento para transferir información personal al exterior y, por consiguiente, corriéndose el riesgo de que los datos de las personas se vean sujetos a usos que en nuestro régimen no serían permitidos.

10. Diferencias con respecto a los Estándares Iberoamericanos de Protección de Datos Personales: Otro aspecto que merece ser resaltado es que varias disposiciones del proyecto no alcanzan el nivel de protección establecido por los Estándares de Protección de Datos Personales para los Estados Iberoamericanos elaborados por la Red Iberoamericana de Protección de Datos Personales (RIPD)[10].

La RIPD es el órgano que agrupa a las autoridades de protección de datos de la región –entre las que se encuentra Argentina– y en su Encuentro de 2017 en Santiago, Chile, lanzó los Estándares con el objetivo de servir como marco de referencia para la actualización de la legislación en los países miembros. Por lo tanto, podemos decir que los Estándares constituyen el consenso iberoamericano sobre cómo deben protegerse los datos de las personas.

Pues bien, existen diversos aspectos dentro del proyecto que pueden ser mejorados en base a dichos estándares, a saber:

a) Incluir los datos biométricos como datos sensibles: el proyecto no incluye a los datos biométricos como datos sensibles, apartándose de este modo de los Estándares. Los datos biométricos –en tanto puedan caracterizar inequívocamente a una persona– gozan de especial importancia, debido a que su utilización implica no solamente una invasión a la privacidad sino también al cuerpo de las personas. Es por ello que su tratamiento debe estar sujeto a estándares tan estrictos como sólo lo puede brindar su caracterización como dato sensible. Por lo tanto, resulta necesario incorporarlos expresamente como tal.

b) Especificar el principio de finalidad: A través de este principio, se busca que el tratamiento de los datos se vea limitado únicamente a aquellos propósitos que el responsable determinó de manera explícita. Además de estos, las legislaciones suelen considerar compatibles otro tipo de tratamientos en consideración al beneficio público que pueden brindar. Tales son los casos de los tratamientos con

[9] Los países considerados con nivel adecuado de protección de datos son: Estados miembros de la Unión Europea y miembros del espacio económico europeo (EEE), Confederación Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá sólo respecto de su sector privado, Principado de Andorra, Nueva Zelanda, República Oriental del Uruguay y Estado de Israel solo respecto de los datos que reciban un tratamiento automatizado. Ver art. 3 de la Disposición 30/16 de la Dirección Nacional de Protección de Datos Personales, disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm (último acceso: 11/10/2018). La lista puede ser revisada periódicamente por la autoridad para incluir o excluir países.

[10] Los Estándares pueden ser consultados en https://bit.ly/2Q68tQu (último acceso: 11/10/2018)

fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Estos casos, por otro lado, suelen estar previstos de manera expresa.

Sin embargo, el proyecto considera que el principio de finalidad también es respetado en el caso de "fines que pudieron ser, de acuerdo al contexto, razonablemente presumidos por el titular de los datos" (art. 6, proyecto de ley). Esta última disposición es sumamente problemática en tanto su vaguedad habilita nuevamente un manejo discrecional por parte del responsable, quien no solamente podrá usar los datos para los fines que haya establecido expresamente sino también ampararse en otros fines que, según él, el titular pudiera de manera razonable haber presumido. Por otro lado, se perjudica el derecho del titular a conocer cómo serán tratados sus datos, ya que no podrá confiar en que su información será manejada solo para aquellos fines que le fueron comunicados explícitamente sino también para cualquier otro propósito que se crea él debió conocer.

Finalmente, el enunciado entra en contradicción con la primera parte de la norma. Si se exige que el propósito sea explícito y determinado, resulta ilógico que luego se permitan finalidades que no son ni explícitas ni determinadas. Por ello, resulta conveniente eliminar la referencia final para ajustarla a los Estándares, en donde no aparece ninguna excepción en ese sentido.

c) No aplicar la condición de "interés legítimo" para justificar el tratamiento de datos por parte de autoridades públicas: Como mencionamos antes, el anteproyecto establecía que esta condición no podía ser invocada por las autoridades públicas, en línea con lo establecido en los Estándares. Sin embargo, esta restricción fue eliminada en el proyecto enviado al Congreso. Debido a lo dicho antes, es aconsejable que esta restricción al manejo discrecional del Estado vuelva a ser incluida.

d) Cambiar el momento en que se debe informar el origen de los datos cuando no fueron obtenidos directamente del titular: Tanto el proyecto como los Estándares establecen el deber de los responsables de comunicar a los titulares de los datos el origen de sus datos cuando no fueron obtenidos directamente de aquellos. Sin embargo, existe una gran diferencia: en los Estándares, dicha obligación existe como parte de la información que se debe proveer al titular previo a la toma de cualquier decisión respecto al tratamiento al que se verá sometido. En cambio, en el proyecto de ley dicha obligación forma parte de la información que debe proveerse luego de un pedido del titular en base al derecho al acceso (art. 28 del proyecto de ley).

De esta manera, aplicando los Estándares obtenemos un mayor nivel de protección para las personas, pues el deber de informar aplica *per se* a todo tratamiento de datos que se lleve a cabo, al no necesitar una conducta activa por parte del titular. Por el contrario, el proyecto expresa que el responsable del tratamiento tendrá el deber de informar únicamente cuando haya una solicitud en ese sentido por parte del titular.

Como corolario, seguramente serán pocos los casos en que este deber se llevaría a cabo en comparación con los que tendrían lugar si se siguieran los Estándares. Así, se perjudica la transparencia

y el acceso a la información por parte de las personas, que merecen conocer de qué forma sus datos fueron obtenidos por responsables a los cuales no les brindaron tales datos. Por lo tanto, el proyecto debería establecer la obligación de informar el origen de los datos en todos los supuestos, sin necesidad de esperar un pedido de acceso del titular.

e) Incluir el derecho a la oposición al tratamiento de datos con fines de marketing o venta directa: Una de las principales herramientas de defensa que brindan los Estándares es la posibilidad de ejercer el derecho de oposición a que los datos personales sean usados para actividades de marketing directo, incluida la elaboración de perfiles. De esta manera, las personas pueden evitar verse sometidas al envío constante de publicidad no deseada y a que se realicen perfiles acerca de su conducta o patrones de consumo, los cuales pueden ser empleados para otros fines o cedidos a terceros.

Esta protección está ausente en el proyecto de ley, ya que no hay ninguna disposición expresa que consagre esta facultad para el titular del dato. Existe la posibilidad de adherirse al Registro No Llame[11], aunque esto solo aplica para los servicios de telefonía y no parece cubrir la elaboración de perfiles. Debido a esto, sería necesario despejar toda duda y consignar expresamente una disposición que permita oponerse a este tipo de prácticas tan habituales y molestas para las personas.

La intención de consagrar un sistema de protección de datos personales adecuado para la era digital resulta un objetivo loable. Sin embargo, esta meta puede verse perjudicada si no se reforman algunas disposiciones del proyecto que entran en tensión con una visión protectoria de los derechos de las personas. En este sentido, desde la ADC comenzamos con el análisis de la iniciativa, a los fines de proponer sugerencias que ayuden a mejorar el proyecto cuando sea discutido por el Congreso.

[11] El Registro No Llame reúne los números telefónicos de las personas que no quieren recibir llamadas publicitarias. Para más información, consultar en http://www.nollame.gob.ar/