Comentarios al anteproyecto de Ley de Protección de Datos Personales

Resumen

Este documento contiene los aportes de los equipos interdisciplinarios de la Fundación Sadosky al anteproyecto de Ley de Protección de Datos Personales presentado por la Agencia de Acceso a la Información Pública en septiembre de 2022.

Está dividido en sugerencias generales y comentarios específicos a nivel de detalles. Los más importantes de estos últimos se encuentran agrupados en la sección Principales aportes. Nos enfocamos en nuestras áreas de especificidad, en particular sobre los conceptos de anonimización, explicación adecuada, seguridad, control humano significativo y procesamiento automático.

Índice

Sobre la Fundación Sadosky

La Fundación Sadosky es una organización público-privada dentro de la órbita del Ministerio de Ciencia y Tecnología de la Nación, cuya misión es la articulación para la innovación productiva en el sector TIC. Cuenta con equipos interdisciplinarios con amplia experiencia en distintas áreas relacionadas con la Informática y está comprometida a contribuir con el desarrollo del país desde su especificidad temática.

La Fundación sigue con atención el proceso de reforma de la Ley de Protección de Datos Personales. Considera que se trata de un proceso muy necesario para nuestro país y valora muy positivamente las mesas redondas, los foros de discusión y el proceso de consulta que la Agencia de Acceso a la Información Pública está llevando adelante como forma participativa de generar consensos alrededor de la nueva ley. La propuesta de anteproyecto fue analizada en conjunto por los equipos de Ciencias de Datos e Inteligencia Artificial, de Seguridad en TIC, de Legales y del área de TIC para la Paz, la Justicia y las Instituciones Sólidas. En este análisis intervinieron investigadoras, investigadores y profesionales de la Informática, de las Ciencias de Datos y del Derecho, entre otros.

Sobre este documento

Este documento es el resultado del debate de los equipos científicos y profesionales multidisciplinares antes mencionados, en conjunción con la dirección ejecutiva de la institución, y expertas y expertos convocados específicamente. La decisión ha sido centrarse en los aspectos en los que, por el perfil de nuestra organización, tenemos más para aportar, en el entendimiento de que también participarán de esta consulta otras organizaciones cuya área de conocimiento se complementará con la nuestra.

Los aportes que a continuación se enumeran deben leerse como propuestas a mejorar un borrador específico, evitando la tentación de realizar una reescritura o propuesta sustantivamente diferente. Más específicamente, el borrador propuesto apunta a señalar un rumbo de prácticas deseables y una infraestructura legal que sirva para que la ciudadanía pueda presentar reclamos ante posibles violaciones, pero no uno que impida de raíz que tales situaciones abusivas se configuren. Tales cambios requerirían un rediseño radical de la norma, lo que entendemos, no es viable en este momento.

A su vez, hemos tratado de que nuestros aportes pongan en primer plano el ejercicio de derechos por parte de la ciudadanía, dando lugar a la innovación tecnológica en el ecosistema de datos. Consideramos que ambas cosas son posibles en la mayoría de los casos, y que debe primar la protección de los derechos cuando se detecten incompatibilidades. Las mejores sociedades son las que más garantías ofrecen a sus ciudadanos y ciudadanas.

Principales aportes

Resumimos aquí los principales aportes de nuestro equipo:

1. Proponemos darle a los **datos derivados** un nivel de protección tan alto como el dato de base sobre el que estén construidos.

2. Proponemos **limitar los usos científicos, históricos, estadísticos y de archivo de los datos, cuando van más allá del consentimiento original**, **agregando condiciones específicas** para cada uno de estos casos y requiriendo tratamientos especiales.

3. Proponemos el concepto de **explicación adecuada** para denominar a las que deberían darse sobre los términos y condiciones: deberían ser claras considerando el público objetivo y que, adicionalmente a las versiones completas, deberían ofrecer versiones abreviadas pero no ingenuas de estos mismos términos y condiciones. Es decir, que sean explícitas sobre puntos que podrían ser de interés para los Titulares de los datos, como por ejemplo, que serán transferidos fuera de su dispositivo, que podrán cederse, etc.

4. Proponemos mantener el **registro de bases de datos**, aunque limitando a aquellas que contengan **datos sensibles**.

5. Dado que la **real anonimización** de los datos es prácticamente imposible (lo explicamos en más detalle en la sección siguiente), realizamos varias propuestas que tienden a **acotar los usos de datos anonimizados por fuera del consentimiento original**.

6. Entendemos que **no deben incluirse excepciones a las bases legales para el tratamiento de datos personales basadas** en la formulación de **intereses legítimos** del responsable del tratamiento de los datos. Cualquier finalidad legítima debe estar claramente abarcada por la presente ley.

7. Si bien es razonable que los **requerimientos específicos sobre seguridad** no queden plasmados en la ley por el riesgo de rápida desactualización, entendemos que no deben quedar abiertos a interpretación y que **debe ser responsabilidad de la AAIP la formulación de normativa específica** que evolucione a la par de la tecnología.

8. En cuanto al **procesamiento automático**, creemos que lo que debe **limitarse es la posibilidad de decisiones para las cuales no se puede, por un lado, asegurar control humano significativo en la toma de decisiones, y por otro aquellos para los que no se puedan proveer explicaciones que los Titulares puedan efectivamente comprender**. En relación al control humano significativo sugerimos una serie de fuentes de información que provienen de instituciones internacionales que se encuentran en el proceso de generar regulaciones para sistemas automatizados. Con respecto al segundo punto, corresponde limitar entonces

aquellas decisiones que se producen a partir de procesos de los cuales no se puede extraer la lógica de funcionamiento y criterios específicos, de manera que puedan ser explicada a los Titulares tanto al momento de consentir al tratamiento de datos personales como luego de que la decisión ha sido tomada y el Titular requiere dicha explicación.

Sugerencias generales al texto de la ley

a. Consideramos que hay algunas medidas protectivas que podría ser interesante requerir a Responsables de mayor envergadura, pero pondrían un umbral muy alto para aquellos de tamaño pequeño. A su vez, las multas que podrían ser significativas para un Responsables de tamaño medio y cumplir su rol de desincentivar las violaciones a la ley, podrían ser analizadas como un pequeño costo para entidades de otro volumen. Por eso proponemos diferenciar las obligaciones de acuerdo al tamaño del Responsable. Este podría ser un camino para indicar una base mínima de protección para todos los casos, que fuese creciendo a medida que crece la capacidad técnica y económica de quien hace el tratamiento.

b. En muchos casos comenzar a utilizar una aplicación o sistema informático importa de parte del titular una decisión con consecuencias duraderas. Se realiza una inversión en dicho sistema, en tiempo de capacitación, en procedimientos, etc. Muchas veces, incluso en identidad (por ejemplo, cuando se publicita el id que alguna plataforma asigna a un usuario, como forma de contacto). Un cambio en esos términos y condiciones cuyo rechazo impide continuar utilizando el servicio deja al titular en situación de indefensión, lo enfrenta ante la posibilidad de perder esa inversión que mencionamos anteriormente o incluso de perder ese identificador identitario que difundió y que eventualmente adoptó casi como parte de su identidad pública. Por ende, consideramos que debería dársele al titular la posibilidad de gozar de términos y condiciones similares a los que aceptó al suscribirse a un servicio, por un periodo determinado. Una propuesta es que ese periodo sea de al menos 5 años.

c. Coincidimos en que hoy en día cualquier tipo de emprendimiento digital, público o privado en el que se registran usuarios, construye una base de datos personales y por ende se pierde el sentido de hacer que deban registrarse. Sin embargo, en el caso de los datos sensibles la situación es distinta. Se trata de una minoría de las bases de datos con información personal y la sensibilidad de la información que contienen justifica un mayor nivel de protección. Por ende, sugerimos mantener la obligación de registrar las bases de datos sensibles.

Comentarios detallados al anteproyecto de ley

Artículo 2

a. En cuanto a la definición de **Anonimización**: Advertimos que en ningún caso es posible garantizar una anonimización completamente irreversible. En base a esto, observamos que los esfuerzos y plazos que se podrían requerir para un proceso de des-anonimización dependerán de los recursos de los cuales se disponga. Es decir, el estado del arte en la tecnología permite que, en la práctica, dependiendo de quién es el actor y cuáles son sus capacidades tecnológicas y económicas, sea posible re-identificar a las personas en muchos casos de interés.

   En cuanto a la redacción del artículo, no queda claro que los esfuerzos a los que se refiere tienen que ver con el proceso de des-anonimización. Por este motivo, más adelante sugerimos que la mera anonimización no sea condición suficiente para bajar el nivel de protección de los datos, y que sólo pueda hacerse en contexto específicos, con fines específicos.

b. Sugerimos eliminar el concepto de **Seudonimización** ya que no se utiliza en el resto del texto.

c. Definición de **Autodeterminación informativa**: A partir de la frase “Comprende un conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales.” Consideramos necesario indicar cuáles o hacer referencia al presente documento si es que hace referencia al conjunto de principios y garantías que esta ley incluye.

d. La definición de **Consentimiento** es innecesaria porque ya está en el artículo 13.

e. Sugerimos cambiar la definición de **Base de datos** por la de *base de datos personales* para que no colisione con el concepto más genérico del mundo de la informática, es decir, el de un conjunto ordenado de datos de cualquier tipo. Así mismo, proponemos cambiar la notificación:

   Base de datos personales: cualquier conjunto de datos personales. Alternativamente podría ser: una colección sistematizada/organizada de datos personales. Desalentamos el uso del adjetivo “estructurada” ya que técnicamente tiene implicancias sobre el tipo de dato al que hace referencia la colección.

   El listado de potenciales formatos y tratamientos solapa con la propia definición de Tratamiento de datos personales que se encuentra más adelante, lo cual hace confusa la comprensión del concepto.

f. Datos genéticos: esta definición difiere de la definición de datos genéticos aprobada por la UNESCO en 2003 en la "Declaración internacional sobre datos genéticos humanos". Dicha definición es la siguiente:

   Datos genéticos humanos: información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos.

Más allá de esta diferencia, sugerimos de cualquier manera eliminar la frase “obtenidos en particular del análisis de una muestra biológica” ya que a nuestro entender reduce el espectro de análisis y herramientas científicas que pueden utilizarse para obtener esta información (por ejemplo, por inferencia genética).

g. La definición de **Entidades crediticias** debería incluir billeteras virtuales para que quienes usan esta forma de servicios de pago digitales no queden por fuera de los alcances de la protección de la ley.

h. Definición de **Tratamiento de datos**: en el listado de operaciones donde dice “de manera enunciativa”, debería agregarse “y no taxativa”.

i. Sugerimos incluir la definición de **datos derivados**: Cualquier dato dentro de la categoría de datos personales que se infiere de otros datos personales propios o no del titular y con cualquier nivel de certeza (inferencias probabilísticas). Estos datos deberían mantener el mismo nivel de protección que el nivel de protección más alto de los datos a partir de los cuales se deriva, ya que si no derivar un dato sensible de otro sería una forma de escapar a los alcances de la ley.

j. En reiteradas oportunidades a lo largo de la ley se utilizan los términos “**fines estadísticos, históricos y científicos**”. Dado que en la mayoría de los casos estos conceptos aparecen relacionados a excepciones donde no aplica la ley o artículos particulares de la misma, sugerimos definirlos concretamente en este artículo y delinear los alcances específicos de cada uno como así también analizar aquellos casos en los cuales los tratamientos incluyan combinaciones de estos tres tipos de finalidades excepcionales. En el caso de los **fines científicos** sugerimos definirlos como/restringirlos a: investigaciones científicas llevadas a cabo en el marco de una institución científica y, cuando corresponda, avalada por un comité de ética. Proponemos incluir la investigación histórica ya que es un tipo particular de investigación científica.

   En el caso de **fines de archivo**, sugerimos diferenciar entre archivo por requerimientos de guarda legal y archivo histórico con fines científicos. En ambos casos consideramos de importancia definir los requerimientos que deben cumplirse para el acceso al archivo en instancias futuras.

   En el caso de **fines estadísticos**, en particular cuando el Responsable no es una institución estatal, nos parece alarmante que esta finalidad, que no está del todo especificada, permite excepciones importantes a la protección de los Titulares de los datos (por ejemplo para el tratamiento de datos sensibles o la no procedencia de la supresión). Sugerimos dar una definición clara y restringida de estos fines.

k. Proponemos la incorporación del concepto de **Explicación adecuada** para referir a cualquier tipo de información que tiene como destinatario el Titular de datos en relación al tratamiento de sus datos personales. Sugerimos utilizar la definición que aparece en el párrafo 4 del artículo 18 como base: “La información sobre el tratamiento de datos debe ser brindada de forma simple, clara y accesible, considerando las características físicomotoras, perceptivas, sensoriales, intelectuales y mentales del usuario, con el uso de recursos audiovisuales cuando corresponda, con el fin de brindar la información necesaria y adecuada a la

comprensión del destinatario". Un ejemplo de una explicación adecuada podría ser incluir a primera vista una versión resumida básica pero no ingenua de los datos que se toman y la opción de ir conociendo progresivamente términos y condiciones.

Artículo 3

a. A nuestro entender el párrafo que comienza con "Se deberá conciliar…" debería ser eliminado. La protección de las fuentes periodísticas tiene protección específica en el art. 43 de la Constitución Nacional y en el art 13 de la Convención Americana de Derechos Humanos. Aún cuando el Congreso Nacional adeuda una ley específica en la materia, es vasta la jurisprudencia referida a los alcances de la protección de los derechos relacionados con la protección de fuentes periodísticas y la libertad de prensa. No es menester de esta ley ofrecer una solución para el sopesamiento de derechos que pudieran entrar en conflicto, sino que esa cuestión interpretativa de la aplicación de la ley es función del poder judicial.

b. Con respecto al párrafo final: "Tampoco serán aplicables las disposiciones establecidas en esta Ley a la información anónima ni a los datos anonimizados de forma tal que el titular de los datos no sea identificable." Sugerimos que no es condición suficiente un proceso de anonimización sobre un conjunto de datos personales para excluirlos de la aplicación de la ley, ya que es imposible probar la imposibilidad de una reidentificación. Esta cláusula de exclusión debería incluir además condiciones específicas sobre los fines particulares del tratamiento. Es decir, en los casos en los que se propone la anonimización como argumento para permitir excepciones a la ley, también deben hacerse requerimientos en cuanto a los fines del tratamiento de datos.

Artículo 6

a. Sería conveniente separar los conceptos de transparencia de explicación. La transparencia debería enfocar en que los procesos de tratamiento de datos personales sean trazables y auditables, mientras que un principio de explicación haría referencia a que se transmita al titular la información referida a sus datos personales de manera clara y sencilla (ver comentario al artículo 2, inciso k).

Artículo 7

a. Habiendo incluido la definición de fines estadísticos, fines de archivo históricos y fines científicos (ver comentario al artículo 2, inciso j). En este artículo sugerimos restringir estas excepciones de la siguiente manera:
    - Fines estadísticos: siempre y cuando estén anonimizados.
    - Fines de archivo: limitar a los tiempos de guarda requeridos para cumplir con requisitos legales que regulan al Responsable.
    - Fines de investigación científica: acreditada de manera legítima (ver comentario tal y cual) y con datos anonimizados.

Artículo 9

a. Sugerimos reformular para definir explícitamente responsabilidades: quien realice el tratamiento de los datos personales sensibles debe asegurarse de que los mismos sean veraces, exactos, completos, comprobables y actualizados. El titular tiene el derecho a reclamar por la veracidad de sus datos, pero no la responsabilidad de mantenerlos actualizados

Artículo 10

a. Consideramos que debe eliminarse el segundo párrafo, ya que los fines indicados como excepción han sido previamente contemplados.

b. Consideramos importante enfatizar la necesidad de no almacenar datos más allá de lo estrictamente necesario, porque esto conlleva altos e injustificados riesgos.

Artículo 11

a. Donde dice “tratamiento adecuado", se debe agregar “a los principios y garantías de la presente Ley”. La narrativa actual puede dejar a libre interpretación el concepto de adecuado, cuando el objetivo sería que es exactamente esta ley la que provee una definición exacta de lo que es adecuado y lo que no.

Artículo 12

a. Consideramos que el inciso d debería ser más restrictivo para evitar abusos por parte de los Responsables.

b. Consideramos también que el inciso f no debería existir. Entendemos que no puede haber intereses de los Responsables que sean estimados por encima de los derechos del Titular. Cualquier finalidad que no esté capturada por los incisos b,c,d, y e, deberían ser abordados siempre con el consentimiento del titular.

c. Bajo nuestra interpretación los datos personales que puedan provenir de sistemas de audio y video vigilancia en la vía pública no quedan bien tipificados en estas bases; deberían incluirse con un criterio restrictivo y razonable. Para los casos donde estos sistemas recolectan datos personales en lugares privados debería darse el consentimiento del titular.

Artículo 13

a. Consideramos que el término “clara acción afirmativa” no es suficientemente objetivo. Si por ejemplo un comercio tuviese cámaras de seguridad, ¿cómo debería ser la acción de los consumidores para que esté avalado que sean filmados?

   En los casos en que se utilicen carteles o notificaciones visuales, creemos que sería oportuno tomar como referencia la ley antitabaco, la ley de etiquetado frontal y la reglamentación sobre carteles de Precios Cuidados. Es decir, normas que procuran mediante la estipulación de tamaños mínimos y ubicaciones que ciertas leyendas no tengan un lugar marginal o que se confundan entre mucha otra información.

   Por ejemplo, un local tiene un cartel que dice “este local tiene cámaras de filmación”. ¿Cómo debería ser ese cartel para asegurarnos de que las personas puedan verlo? ¿En qué ubicación debería estar colocado?

b. En la definición de Libre: proponemos quitar la segunda oración. Consideramos que habrá muchos casos en los que el Titular puede sufrir perjuicios por negarse a otorgar su consentimiento. Por ejemplo, el perjuicio de no poder participar de una actividad, o utilizar un servicio, o ingresar a un establecimiento para acceder a algo que necesita o desea realizar. En un caso así, el Titular es libre de elegir entre dar su consentimiento o no, pero es claro que podría suceder que por negarse sufrirá un perjuicio.

Artículo 14

a. Al final del artículo consideramos pertinente agregar que debe ser posible la revocación por el mismo medio por el cual se dio el consentimiento

b. No es claro cómo afecta la revocación en aquellos actores a quienes el Responsable del tratamiento le transfirió los datos personales del Titular. Sugerimos que se exija una revocación en cascada a cargo del Responsable y que bajo ninguna circunstancia implique un impedimento para que el titular pueda ejercer su derecho (por ejemplo, no sería razonable que sea el propio titular quien deba contactar a las diferentes entidades a los que sus datos fueron cedidos o transferidos para revocar el consentimiento al tratamiento).

Artículo 15

a. Usar una definición de accesible, sencillo y claro basada en la propuesta del concepto de explicación (ver comentario al artículo 2, inciso k). Un ejemplo de una explicación adecuada podría ser incluir a primera vista una versión resumida y jerarquizada de la información que se debe presentar al Titular de manera que el Titular pueda de forma inmediata reconocer el alcance de la cesión de sus datos. Ejemplo: al usar software de terceros que requieran información de un usuario (Titular) en Google, este presenta una lista con los datos y accesos que se le proveerán, al lado de un link con la información detallada.

b. En el inciso b las categorías son aquellas definidas en el artículo 2, de manera enunciativa y no taxativa.

c. En el inciso j incluir “los criterios y procedimientos utilizados (ver art. 30)”

d. En el anteúltimo párrafo: “Cuando los datos no hayan sido obtenidos del Titular, el Responsable deberá proveer la información prevista en el presente artículo dentro de un plazo razonable y a más tardar dentro de un mes.” No queda claro el plazo y las condiciones en que esto debería suceder.

Artículo 16

a. Inciso d: esta excepción debe estar limitada a la actividad particular de la asociación (por ejemplo, no hay razón para que una organización sindical haga tratamiento de datos personales sobre preferencias religiosas).

b. En el inciso f, restringir en los mismos términos que se sugirieron en el comentario al artículo 7.

   Quitar la calificación “En la medida de lo posible” respecto de la anonimización.

Artículo 18

a. Nuestra sugerencia es que este artículo debería ser mucho más estricto y taxativo.

b. Revisar inciso 2, no parece adecuada la frase “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 el menor o adolescente, teniendo en cuenta sus posibilidades para hacerlo.” Se debe pensar y proponer (quizás desde lo normativo), un procedimiento que permita efectivamente la validación sin contribuir a la creación de nuevas bases de datos personales. La utilización de un sistema/base de datos como Mi Argentina podría ser una opción. Pero esa frase no debería aparecer en la presente ley.

c. No es claro el propósito del inciso 6, sugerimos revisar o eliminar.

Artículo 19

a. El primer párrafo no es claro, es circular porque nunca se provee una definición de seguridad.

b. Segundo párrafo, se habla de las medidas de seguridad preventivas y correctivas que deberán adoptarse pero no se especifica cuáles serán estas medidas. Sugerimos incluir que dichas medidas preventivas y correctivas serán definidas por la autoridad de aplicación de la presente ley en adición a las que determine el organismo de control competente de acuerdo al sector de actividad. Deberá

considerarse en carácter incremental de acuerdo al volumen de transacción de datos personales.

c. Se habla de riesgo sin embargo no se establece qué modelo debe seguirse para computar dicho riesgo. Podría introducirse un modelo básico (ej., probabilidad de ocurrencia x impacto) o bien dejar dicho explícitamente que los riesgos de los que se habla a lo largo del documento seguirán un modelo de riesgo determinado por la autoridad de aplicación.

d. Dentro de este artículo se debería exigir la presentación de un análisis de riesgo formal (de acuerdo al modelo de riesgo que la autoridad de aplicación determine).

e. Es importante agregar que cuando se presente un incidente, este debe ser documentado e informado también a la AAIP.

Artículo 20

a. Primer párrafo, sugerimos cambiar el lapso de tiempo para informar por 72 horas. Consideramos que 48 horas puede ser muy restrictivo en muchos casos prácticos. Dependiendo de diversos factores que pueden estar relacionados con el tipo y tamaño de la organización, puede suceder que se deben llevar a cabo una serie de procesos no triviales al momento en que se detecta un (potencial) incidente no solo para poder entender la magnitud del incidente y los posibles datos y/o sistemas comprometidos sino también relacionados con cuestiones legales procesos internos que requieren comunicación entre diversos actores . Nuestra sugerencia es que se le de a la organización 72 horas para poder realizar la primera comunicación con el Titular acerca del incidente.

b. Segundo párrafo: recomendamos eliminar términos como “probable” o “altos” riesgos. Por un lado son términos subjetivos y la ley no prevé dispositivos para estipularlos de manera concreta. Por otro lado, consideramos que es importante que **todos** los incidentes que puedan comprometer los datos personales de un Titular sean informados lo antes posible. Muchas veces en la práctica, no es posible determinar con exactitud (o aproximar con una precisión aceptable) la magnitud de los efectos de un incidente de seguridad hasta pasado cierto tiempo, probablemente muy superior al lapso de tiempo previsto en el primer párrafo de este artículo. Recomendamos reformular, indicando que el Responsable debe informar al Titular **siempre que suceda un incidente de seguridad** de datos personales según la definición de incidente de seguridad establecida en el artículo 2.

   Entendemos que esta sugerencia puede llevar en algunos casos a sobrecarga, por lo que sería adecuado que en la normativa que acompañe esta ley se establezca una manera de definir un umbral adecuado, definido por la agencia de aplicación, para evitar estas situaciones.

c. Tercer párrafo: recomendamos quitar el término “esfuerzo desproporcionado”. Las buenas prácticas de seguridad indican que al titular se le debe informar cuando no se puede descartar que sus datos pueden haber sido comprometidos. Esto es, si no

es posible definir exactamente quienes fueron afectados, la obligación es informar a todos los Titulares de los datos.

Artículo 22

a. Sugerimos que todo el listado de supuestos deba cumplirse para poder efectivamente realizar transferencias de datos personales dentro del marco de esta ley. Esto es, el primer párrafo debería decir: “Las transferencias de datos personales fuera del territorio nacional, incluidas las transferencias ulteriores se podrán realizar en el caso en que se cumplan los siguientes supuestos de manera conjunta:”

b. En el inciso a, sugerimos cambiar “adecuado” por “equivalente o superior a la protección requerida en las leyes nacionales”.

c. Asimismo sugerimos aclarar que si el país u organismo dejare de cumplir con estos supuestos, se revocará la autorización y deberán eliminarse los datos transferidos.

Artículo 23

a. En concordancia con las modificaciones sugeridas para el artículo 22, en este caso habría que reemplazar “condición de adecuado” por “condición equivalente”.

Artículo 26

a. En el inciso i: Consideramos innecesario decir “sin que ello afecte derechos intelectuales del Responsable del tratamiento”.

   Creemos que es razonable requerir al Responsable de los datos encontrar la manera de explicar las reglas utilizadas para la toma de decisiones sin que esto implique un descuido de la propiedad intelectual.

b. Tanto en el inciso i como en el último párrafo, sugerimos dar mayor especificación sobre el suministro adecuado de la información. (Ver comentario al artículo 2, inciso k).

Artículo 28

a. En el primer párrafo es pertinente aclarar que la excepción al derecho de oposición debe ser en únicamente en términos de los motivos que establece el artículo 12 (incisos del b al f).

Artículo 29

a. Luego del inciso f, donde se tratan las excepciones para la supresión:

   Donde dice “no procederá cuando pudiese causar perjuicios a derechos o intereses legítimos…” sugerimos omitir “intereses legítimos”. Consideramos que los intereses de terceros no deben anteponerse a los derechos del Titular.

   En el anteúltimo párrafo, referimos a la sugerencia hecha previamente (ver comentario al artículo 2, inciso j) en relación a los fines estadísticos, de investigación científica, o históricos. Sugerimos evitar la frase “siempre que no pudiera aplicarse el proceso de anonimización”.

Artículo 30

a. En el primer párrafo sugerimos:

   El titular de los datos tiene derecho “a” no ser objeto de decisiones automatizadas o semiautomatizadas salvo en los términos estipulados en el Artículo 12.

   Proponemos eliminar la frase “que le produzca efectos jurídicos perniciosos, lo afecte significativamente de forma negativa o tenga efectos discriminatorios” porque implica una inversión en la carga de la prueba. Entendemos que este derecho debe poder ser asegurado sin condición y que cualquier actividad que perjudique al titular no sería legal dentro de lo estipulado en el artículo 12 (entendiéndolo bajo las sugerencias marcadas previamente en el comentario al artículo 12).

b. En cuanto al resto del artículo, proponemos una reformulación, de modo que el objetivo de este artículo garantice i) **control humano significativo** y ii) **explicaciones adecuadas** en relación a los tratamientos y las decisiones que se toman en base a estos.

   Con respecto a i), el Responsable de los datos debe poder garantizar un **control humano significativo** sobre los procesos automatizados que trabajan sobre datos personales. El concepto de control humano significativo se propone en la literatura como un intento de abordar las brechas de responsabilidad en el desarrollo y uso de sistemas automatizados[1]. La finalidad de esta formalización es poder establecer condiciones que permitan una adecuada atribución de responsabilidad a los humanos en todo el ciclo de vida del sistema. En este caso particular, por cada decisión que se toma sobre el Titular de los datos debe existir siempre una persona humana responsable de dicha decisión (en términos civiles, penales y de las garantías y derechos contenidas en esta ley), no pudiendo adjudicarse al “sistema” la toma de la misma. Es importante destacar que la garantía de mantener un control humano significativo sobre la toma de decisiones evitaría, en principio, el tratamiento de datos personales por medio de procesos de “caja negra”, es decir sistemas no interpretables o con baja transparencia.

[1] Cavalcante Siebert, L., Lupetti, M. L., Aizenberg, E., Beckers, N., Zgonnikov, A., Veluwenkamp, H., ... & Lagendijk, R. L. (2022). Meaningful human control: actionable properties for AI system development. AI and Ethics, 1-15.

Con respecto a ii) las decisiones alcanzadas en base al tratamiento de los datos personales **deben poder ser siempre explicadas** de manera adecuada (de acuerdo al concepto de explicación sugerido previamente en el comentario al artículo 2, inciso k), no pudiendo entonces utilizarse implementación de las cuales no se pueda obtener la lógica de funcionamiento y los criterios específicos utilizados para tomar la decisión. A su vez, en estos casos, cada explicación de esta decisión debe poder ser reproducible por un humano. Es decir, los sistemas automatizados pueden usar su poder de cómputo y sus algoritmos sofisticados para "encontrar la aguja en el pajar", pero luego debe producirse, de manera automática o humana, una explicación veraz y comprensible de por qué eso que se encontró, es efectivamente "la aguja buscada".

c. Omitir “observando secretos comerciales e industriales” ya que brinda al Responsable de los datos un argumento no cuestionable para no cumplir.

   Creemos que es razonable requerir al Responsable de los datos encontrar la manera de explicar las reglas utilizadas para la toma de decisiones sin que esto implique un descuido de los secretos comerciales o industriales.

a. Consideramos que además de las auditorías previstas por este artículo es necesario prever sanciones específicas en relación a las decisiones automatizadas y la elaboración de perfiles.

Artículo 31

a. El artículo 31 propone como excepción a la portabilidad diversos casos que consideramos oportunos excepto los mencionados en los incisos:

   - a) cuando “su ejercicio impone carga financiera o técnica excesiva o irrazonable sobre el Responsable…” ya que independientemente de la carga que implique, el Responsable debería poder proporcionar una copia de los datos personales. Este inciso podría dar lugar al uso mal intencionado promoviendo la complejización del tratamiento con el fin de no poder dar la copia que de por sí es de propiedad del Titular.

   - c) “Afecte las obligaciones legales del Responsable…” Consideramos que de llegar este caso, el Responsable debería abstenerse del uso de los datos personales del Titular si esto lo compromete legalmente a sí mismo.

   - d) “Impida que el Responsable del tratamiento proteja sus derechos…” Como en el caso anterior, consideramos que de llegar este caso, el Responsable debería abstenerse del uso de los datos personales del Titular si esto compromete a sí mismo, al Encargado o a terceros.

Artículo 36

a. El concepto de “cambios sustanciales” es subjetivo. Sugerimos solamente decir “cambios”. Entendiendo que el artículo pretende capturar sólo aquellos cambios que pongan en riesgo los principio y garantías que esta ley establece para el Titular de los datos, quizás debería quedar explícito que en la práctica el tipo de cambios que deberán informarse serán definidos por la Agencia de aplicación.

Artículo 37

a. El artículo establece una serie de medidas definidas de manera poco clara, dando lugar a una multiplicidad de interpretaciones de la forma y objetivos que persiguen las mismas.

Artículo 38

a. Consideramos que el artículo 38 apunta a promover la protección de los datos personales y los derechos de los Titulares de los datos por diseño y por defecto, es decir que los procesos que involucran el tratamiento de los datos personales deben ser diseñados de manera tal que no entrañen riesgos o perjuicios a los Titulares de los mismos. De la manera en que está redactado, sobre todo el último párrafo, el foco está solamente en la seguridad de los datos y no parecerìa abarcar el diseño de procesos de tratamientos de datos que puedan producir perjuicios a los Titulares y/o efectos colaterales no deseados. Creemos que sería conveniente clarificar el objetivo del artículo en los términos sugeridos. Esto permitirá promover una acción proactiva en pos de un diseño ético de los procesos de tratamiento de datos personales.

b. No se establecen parámetros sobre las medidas tecnológicas y organizativas que se proponen definir. Debería explicitarse que dichas medidas serán definidas por la Agencia de aplicación.

Artículo 39

a. Remover de los incisos b y c el calificativo “a gran escala” pues creemos que es necesaria la evaluación de impacto sin importar el volumen de los datos tratados. Maliciosamente podrían tratarse pocos datos si al Responsable solo le importa cierto grupo de Titulares. Por otro lado, ¿cuál sería el límite entre pequeña y gran escala? Además, un tratamiento a pequeña escala no garantiza que no pueda existir un efecto negativo a partir del mismo. Tales tratamientos, justamente por su naturaleza de ser realizados sobre “pocos” datos, podrían en principio introducir sesgos sobre el análisis y las conclusiones que se hagan sobre datos personales que podrían repercutir de manera negativa en un sector de la sociedad. Esto debe ser de especial cuidado, pero no limitado, a tratamientos que incluyan procesos automatizados.

Artículos 38 a 40

a. Consideramos que se debería especificar la obligatoriedad de la Autoridad de Aplicación a elaborar pautas específicas.

Artículo 42

a. Creemos que habría que definir claramente los requisitos de idoneidad del Delegado de protección de datos.

b. A su vez, no debería ser sancionado ni durante ni después de sus funciones.

Artículo 44

a. No está claro qué se entiende por un tratamiento ocasional. Si esto incluye situaciones donde el tratamiento es esporádico, ¿qué sucede en los casos en los que estos tratamientos son determinantes o se venden, por ejemplo, a otro Representante? Podemos tomar como ejemplo real, el caso de Cambridge Analytica y su influencia en elecciones políticas. En el año 2013 fue lanzada una aplicación para usuarios de Facebook que mediante un test recababa información sobre la personalidad del usuario junto a datos sobre su comportamiento en la red social y el perfil de todos sus contactos. De esta forma logró generarse una base de datos de unos 50 millones de usuarios en unos pocos meses, los cuales fueron vendidos a la empresa Cambridge Analytica. Hay muchas denuncias de que esos datos privados fueron utilizados para manipular a los votantes en las elecciones de EE.UU. de 2016, con potenciales implicaciones también en varios países latinoamericanos. En este caso, en la primera sesión, el tratamiento fue de una única vez lo que podría entenderse como un tratamiento ocasional y las disposiciones de esta ley no aplicarían.

Artículo 47

a. No debería ser posible el uso de datos sensibles para el caso tratado en el artículo. Entendemos que ese tipo de información no debería ser incluida en un perfil crediticio ni ser utilizada para la toma de decisiones en ese ámbito particular. Si existieran datos sensibles que son absolutamente necesarios para este tipo de actividad, la entidad debería solicitar a la agencia de aplicación una autorización para el tratamiento de los mismos de manera excepcional.

Artículo 48

a. En este artículo sugerimos revisar la redacción ya que no resulta claro.

b. Se menciona que “Sólo se podrán tratar datos personales que sean significativos”, sin embargo, en ningún momento queda definido a qué se refiere con “significativos” en términos crediticios.

c. Proponemos reducir de 1 (un) año a 6 (seis) los meses de conservación de la información crediticia cuando el deudor cancele o extinga la obligación.

d. Los plazos deberían contarse desde el momento en que se evalúa la solvencia, y no depender de la última información significativa.

Artículo 49

a. El artículo establece que “se deberá comunicar detalladamente al Titular de los datos cuál es la fórmula, variables, el procedimiento y la información que tomó en cuenta o el algoritmo que se utiliza y su composición.” Esta comunicación deberá hacerse en los términos de accesibilidad sugeridos en los comentarios al artículo 2, inciso k.

Artículo 51

a. Consideramos que se le asignan muchas funciones y responsabilidades a la Autoridad de Aplicación, y nos preocupa que no se estipulan recursos para el desarrollo de las mismas.

b. En particular en el inciso ñ se sugiere el desarrollo de investigación y conocimiento y siendo conscientes de que los recursos para la investigación en el país son escasos, tampoco se estipulan mecanismos ni recursos para que dicho desarrollo sea viable.

Artículo 53

a. En el primer párrafo se establece que el Titular puede realizar un denuncia acreditando que efectuó la intimación correspondiente. Esto debería considerar la posibilidad de que el Titular no pudiera efectuar la intimación correspondiente porque no existe un contacto o lugar (físico o virtual) donde el Titular pueda dirigir dicha intimación. Lamentablemente este suele ser el caso en muchas oportunidades en la práctica en particular por servicios ofrecidos de manera digital.

Artículo 59

a. Consideramos menester revisar el valor de la unidad móvil en pesos al momento de presentar el proyecto en el Congreso para evitar que quede desactualizado al momento mismo de su creación.

Artículo 60

a. En ningún lugar se indica cuál sería el fin de los fondos provenientes de las multas. En particular, proponemos que el dinero recaudado por las sanciones podría ir a un fondo para actividades de desarrollo sobre los temas objeto de esta ley.

Colaboradores

Colaboraron en este documento:

Fernando Schapachnik

Gustavo Sibilla

Juan Heguiabehere

Laura Marés

Lucas Somacal

Manuela Cerdeiro

Maria Soledad Escobar

Maria Vanina Martinez

Matias Cavanagh

Victoria Gisel Dumas