CÁMARA ARGENTINA DE Internet

Buenos Aires, 26 de Septiembre de 2022

Sra. Directora
Lic. Beatriz De Anchorena
Agencia de Acceso a la Información Pública
S / D

Referencia: Consulta Pública – Actualización de la Ley de Protección de Datos Personales

Me dirijo a Usted, en representación de la Cámara Argentina de Internet (CABASE), en el marco de la Consulta Pública dispuesta por Resolución AAIP 119/2022, con la finalidad de solicitar que la fecha de vencimiento de la misma se extienda al menos 10 días hábiles.

Esta solicitud se fundamenta en la necesidad de contar con mayor plazo para finalizar el análisis del anteproyecto de ley de protección de datos personales sometido a consulta y para concluir la elaboración de los comentarios y sugerencias por parte de la entidad que represento.

En este sentido, desde la publicación de la Resolución AAIP 119/2022, las comisiones internas de CABASE han estado trabajando para responder en tiempo y forma a la misma, pero la longitud del anteproyecto así como los cambios que propone a la legislación vigente, ameritan un pormenorizado análisis y evaluación.

Entendemos que 10 días hábiles, a contar desde el 30 de Septiembre serán suficientes para poder efectuar los comentarios y observaciones que el proceso de Consulta Pública requiere.

Sin otro particular, la saludo a Usted muy atentamente.

Ing. Ariel Graizer
Presidente
Cámara Argentina de Internet- CABASE

Cámara de Informática y Comunicaciones de la República Argentina

CICOMRA

Buenos Aires, 27 de Septiembre de 2022

Señora Directora
Agencia de Acceso a la Información Pública
Mg. Beatriz de Anchorena
Presente

Ref.: Solicitud de Prórroga - Resolución 119/2022 - Consulta Pública sobre "PROPUESTA DE ANTE PROYECTO DE LEY PROTECCIÓN DE DATOS PERSONALES"

De nuestra mayor consideración:

Nos dirigimos a Usted en representación de CICOMRA - Cámara de Informática y Comunicaciones de la República Argentina, con relación a la Consulta Pública establecida en la **Resolución 119/2022** por la Propuesta de Anteproyecto de Ley de Protección de Datos Personales.

Al respecto, y en función al pedido de empresas socias de nuestra cámara, solicitamos por favor tenga a bien considerar extender una prórroga al plazo previsto en la norma mencionada para responder a la Consulta Pública, debido a lo complejo del análisis del Proyecto de referencia.

A la espera de que se considere favorablemente lo solicitado, la saludamos muy atentamente.

Norberto Capellán
Presidente
CICOMRA

capellan@cicomra.org.ar

Asociación Argentina TIC,
Video & Conectividad

Ciudad Autónoma de Buenos Aires, 27 de septiembre de 2022.-

Sra. Directora de la Agencia de Acceso a la Información Pública
Sra. Beatriz Anchorena
S / D

Ref.: Resolución N° 119/2022 AAIP
"Anteproyecto de Ley de Protección de Datos Personales"

De mi mayor consideración:

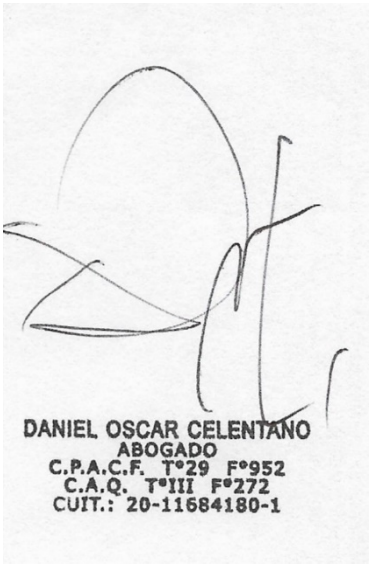
Daniel Oscar Celentano, abogado, Tº 29 Fº 952 (CPACF) con domicilio especial en Avda. de Mayo 749 5º Piso Oficina 31 de la Ciudad Autónoma de Buenos Aires, domicilio electrónico: atvc@atvc.org.ar en representación de la Asociación Argentina TIC, Video & Conectividad (en adelante "ATVC") continuadora de la Asociación Argentina de Televisión por Cable (ATVC) como surge del Poder General Administrativo, Bancario y Judicial que en copia se acompaña y del cual declaro bajo juramento su autenticidad y vigencia tiene el agrado de presentarse ante la Sra. Directora de la Agencia de Acceso a la Información Pública y dice:

Previamente y cumpliendo expresas instrucciones de mis mandantes hago propicia la oportunidad para agradecer a la autoridad la instancia de participación brindada, la cual permite a todos los sectores de la sociedad involucrados, presentar sus opiniones y propuestas sobre el tema de referencia.

En concordancia con lo dicho y dada la magnitud de las implicancias que el Anteproyecto en cuestión podría implicar para los miembros de la Cámara que represento, solicitamos se amplie el plazo para la presentación de dichas contribuciones, en un mínimo de 15 días hábiles.

Cabe mencionar que, si bien la norma en análisis encuentra sus raíces en legislación comparada, resulta imprescindible analizar concienzudamente y a la luz de las distintas disciplinas que involucra esta materia, sus eventuales impactos en el contexto nacional, para así aportar fundadas consideraciones y propuestas.

Quedando a su entera disposición para cualquier aclaración al respecto, aprovecho la oportunidad para saludar a Usted atentamente.



Cámara Argentina de Comercio y Servicios

Buenos Aires, 27 de septiembre de 2022

At.
Sra. Directora
Mg. Beatriz Anchorena
Agencia de Acceso a la Información Pública (AAIP)

S_/_D

***Ref.:* Solicitud de Prórroga**
Propuesta de Anteproyecto de Ley
de Protección de Datos Personales

De nuestra consideración:

Tenemos el agrado de dirigirnos a Ud. en representación de la Cámara Argentina de Comercio y Servicios (CAC) por el asunto de referencia.

Luego del análisis y consultas efectuadas con nuestros socios respecto de la Propuesta de Anteproyecto de Ley de Protección de Datos Personales, publicado mediante la Resolución AAIP 119/2022, es que consideramos oportuno la ***extensión del plazo previsto en la norma mencionada para responder a la Consulta Pública*** allí establecida con motivo de la complejidad del tema que se trata.

A la espera de una respuesta favorable, la saludamos cordialmente.

Rodrigo Pérez Graziano
SECRETARIO

Natalio Mario Grinman
PRESIDENTE

Buenos Aires, 28 de Septiembre de 2022

Sra. Directora
Lic. Beatriz De Anchorena
Agencia de Acceso a la Información Pública
S / D

Referencia: Consulta Pública – Actualización de la Ley de Protección de Datos Personales

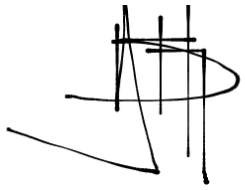
Me dirijo a Usted, en representación de la Cámara Argentina de Comercio Electrónico (CACE), en el marco de la Consulta Pública dispuesta por Resolución AAIP 119/2022, con la finalidad de solicitar que la fecha de vencimiento de la misma se extienda al menos 10 días hábiles.

Esta solicitud se fundamenta en la necesidad de contar con mayor plazo para finalizar el análisis del anteproyecto de ley de protección de datos personales sometido a consulta y para concluir la elaboración de los comentarios y sugerencias por parte de la entidad que represento.

En este sentido, desde la publicación de la Resolución AAIP 119/2022, las comisiones internas de CACE han estado trabajando para responder en tiempo y forma a la misma, pero la longitud del anteproyecto así como los cambios que propone a la legislación vigente, ameritan un pormenorizado análisis y evaluación.

Entendemos que 10 días hábiles, a contar desde el 30 de Septiembre serán suficientes para poder efectuar los comentarios y observaciones que el proceso de Consulta Pública requiere.

Sin otro particular, la saludo a Usted muy atentamente.



Gustavo Sambucetti
Director Institucional
Cámara Argentina de Comercio Electrónico - CACE

Rosario, 29 de septiembre de 2022

Sres.
Agencia de Acceso a la Información Pública
S. / D.

Ref: Comentarios a Resolución 119/2022

De nuestra mayor consideración:

Tenemos el agrado de dirigirnos a Ud. con motivo del Proyecto de Ley de Protección de Datos Personales emitido bajo la Resolución 119/2022, en el marco del procedimiento de Elaboración Participativa de Normas aprobado por el Decreto Nº 1172/2003, el cual fuera objeto de análisis conjunto por Bolsa de Comercio de Rosario, Matba Rofex S.A. y Mercado Argentino de Valores S.A.

En el marco del análisis realizado, celebramos la iniciativa de emitir normas que tengan como fin primordial armonizar los estándares regionales e internacionales en materia de protección de datos personales para fortalecer una estrategia global de regulación, desde un enfoque de derechos humanos y con una mirada situada y soberana, ello impulsado por los nuevos escenarios caracterizados por movimientos constantes de grandes flujos de datos, refuerzan la necesidad de que la República Argentina mantenga los estándares de protección capaces de compatibilizar la economía digital, la innovación tecnológica y la protección de derechos fundamentales, en el marco de un proyecto de desarrollo inclusivo.

De esta manera, como sectores interesados en dicha normativa, venimos a formar parte del proceso de Elaboración Participativa de las Normas a la que el Proyecto de Resolución fue sometido, haciendo llegar nuestros comentarios y sugerencias en el Anexo I, a fin de potenciar la misma.

Quedamos a vuestra disposición y saludamos a Uds. muy atentamente.

Javier E. Cervio
Director Institucional y de Mercados
Bolsa de Comercio de Rosario

Andrés Ponte
Presidente
Matba Rofex S.A.

Alberto Curado
Presidente
Mercado Argentino de Valores S.A.

ANEXO

- **Artículo 2° Definiciones:**

Sobre el detalle de los nuevos conceptos, se sugiere Incorporar los términos *mercadotecnia y prospección comercial* según el alcance dentro de esta ley, tal como los mismos serán considerados según el artículo 28 Derecho de Oposición.

- **Artículo 10° Plazo de conservación:**

"Los datos personales no deben ser mantenidos más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

Los datos personales pueden conservarse durante períodos más largos siempre que se traten exclusivamente con fines estadísticos, de archivo en interés público, de investigación científica o histórica, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone la presente Ley a fin de proteger los derechos del Titular de los datos."

Sugerencia: Para mayor claridad se sugiere establecer plazos definidos para su conservación, dado que la mención de "el tiempo estrictamente necesario para el cumplimiento de la finalidad" puede llegar a inducir a diferentes criterios o subjetividad a la hora de determinarlo.

- **Artículo 13°Consentimiento**

"Cuando la base legal para el tratamiento de datos sea el consentimiento del Titular, se requiere que éste sea previo, libre, específico, informado e inequívoco para una o varias finalidades determinadas, ya sea mediante una declaración o una clara acción afirmativa.

Se entiende por:

1) Previo, cuando se solicita el consentimiento antes de la recolección de los datos;

2) Libre, cuando se encuentre exento de vicios. El Titular de los datos deberá tener la opción de negarse a otorgar su consentimiento sin sufrir perjuicio alguno;

3) Específico, que cuando el tratamiento de datos tenga varios fines, el Titular otorgue el consentimiento para cada uno de ellos;

3) Informado, de modo que el Titular cuente con la información establecida en el artículo 15;

4) Inequívoco, de manera que no presente dudas sobre el alcance de la autorización otorgada por el Titular.

El Responsable deberá ser capaz de demostrar que el Titular consintió el tratamiento de sus datos personales."

Sugerencia: A fin de dar mayor claridad al artículo y tal como se hace en otros, sería conveniente

incorporar en forma meramente enunciativa casos a considerar declaración o una clara acción afirmativa a los fines de tenerse por acreditado el consentimiento en forma tácita.

- **Artículo 21° Deber de Confidencialidad:**

"El Responsable del tratamiento, el Encargado y las demás personas que intervengan en cualquier fase del tratamiento están obligados a la confidencialidad respecto de los datos personales. Esta obligación subsiste aún después de finalizada su relación con el Titular de los datos, el Responsable o el Encargado del tratamiento, según corresponda. El obligado puede ser relevado del deber de confidencialidad por resolución judicial."

Sugerencia: se sugiere, en cuanto al relevamiento del deber, que pueda ser además de por resolución judicial, en analogía con el mismo deber en el ámbito de mercados, que sea cuando fuere solicitado por organismos de contralor como: AFIP, UIF, entre otras, con pedido debidamente fundado y por autoridad competente en cada uno de las mismas en el alcance de sus facultades.

- **Artículo 34°. Responsable del tratamiento – Artículo 35° Encargado de tratamiento - Artículo 42° Delegado de protección de datos.**

"Los Responsables de Tratamiento y los Encargados del tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente Ley, sus normas reglamentarias y otras que rijan su actividad: …."

"Los Responsables y Encargados del tratamiento deben designar un Delegado de protección de datos en cualquiera de los siguientes supuestos:… "

Sugerencia: Del análisis de la norma advertimos que la misma genera 3 nuevos roles a fin de llevar a cabo un control más adecuado para el tratamiento de datos, lo cual en los roles que ya se establecen por diferentes normativas de organismos como la Comisión Nacional Valores y la Unidad de Información Financiera, sumado a la normativa en materia de Integridad, genera ante ciertos actores, la necesidad de contar con multiplicidad de roles en su estructura a fin de dar cumplimiento a lo exigido. Es por ello que se solicita que todas las figuras mencionadas se subsuman en una única a los efectos mencionados.

- **Artículo 39° Evaluación de impacto relativa a la protección de datos**

personales

“Cuando el Responsable del tratamiento prevea realizar algún tipo de tratamiento de datos que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación a los derechos de los Titulares de los datos amparados en la presente Ley, deberá realizar, de manera previa a la implementación del tratamiento, una evaluación del impacto relativa a la protección de los datos personales.

Esta evaluación es obligatoria en los siguientes casos, sin perjuicio de otros que establezca la Autoridad de aplicación:

a. Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado y semiautomatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que les afecten significativamente de modo similar;

b. Tratamiento de datos sensibles a gran escala, de datos relativos a antecedentes penales, contravencionales o de niños, niñas y adolescentes;

c. Observación sistemática a gran escala de una zona de acceso público.

Sugerencia: En primera instancia sería óptimo poder delinear en forma más concreta el alcance de *“… sea probable que entrañe un alto riesgo de afectación*”, pudiendo determinar al menos parámetros que permitan determinar dicha situación.

Asimismo, en cuanto al inciso b, sugerimos determinar en qué casos será considerado tratamiento a gran escala.

Cámara de Tarjetas de Crédito

directorejecutivo@atacyc.com.ar

mar 27/09/2022 04:38 p.m.

Para:Consulta Pública <Consultapublica@aaip.gob.ar>;

Estimados,

Con relación al anteproyecto de ley de Protección de Datos Personales, deseamos informarles que desde ATACYC, cámara que agrupa a las principales empresas emisoras y administradoras de Tarjetas de Crédito y de otros medios de pago electrónicos, estamos trabajando intensamente en el estudio del mismo.

Dada la importancia que tiene este proyecto, el alto impacto que tiene este tipo de regulación en nuestra actividad, y atentos a que está próximo a vencer el plazo para presentar comentarios al mismo, solicitamos una prórroga de al menos un mes para hacer llegar nuestros acotaciones y sugerencias.

Sin otro particular, saludos a Ustedes muy atentamente,

César Bastien
Director Ejecutivo
ATACYC

Buenos Aires, 30 de septiembre de 2022

Mg. Beatriz de Anchorena
Titular
Agencia de Acceso a la Información Pública
S / D

De nuestra mayor consideración,

Me es grato dirigirme a usted a efectos de sumar a Argencon al debate que la Agencia ha propuesto a organizaciones de la sociedad civil, universidades y el sector privado sobre la legislación de protección de datos, tema de especial relevancia para nuestros asociados.

Argencon es la primera entidad del país que nuclea a empresas prestadoras de servicios de todos los verticales de la Economía del Conocimiento. Nucleamos a las empresas del conocimiento con orientación exportadora y liderazgo en sus rubros de actuación. Actualmente, nuestra comunidad de socios está conformada por 45 empresas líderes que integran seis clústeres: Centros de Servicios Globales, Servicios Profesionales, Biotecnología, Empresas de IT, Medios y Tecnología Productiva. La Economía del Conocimiento exporta hoy un valor superior a U$S 7,2 mil millones anuales, y ocupa más del 7% del empleo registrado en el país. Nuestros asociados representaron en 2021 más del 25% del total de las exportaciones nacionales.

Trabajamos para generar las condiciones que favorezcan el desarrollo del sector y la formación de talento digital, además de promover el crecimiento de las exportaciones y el posicionamiento de Argentina como líder en la prestación de servicios del conocimiento a nivel global.

En todas las actividades de la Economía del Conocimiento el tratamiento de datos es intensivo y constituye la esencia del mundo digital. Por tal motivo valoramos muy positivamente la invitación a sumar nuestra opinión al debate que se inicia para actualizar la Ley N°25.326 de Protección de Datos Personales.

En nuestra opinión el modelo argentino de política pública respecto de la Protección de Datos debe converger con el estándar europeo, que es ampliamente aceptado como la norma más adecuada a nivel mundial. La conveniencia de converger sobre un modelo global es lógica, como consecuencia de la naturaleza transfronteriza del uso de los datos. Definir estándares no alineados con esas tendencias supondrá no solo una complicación operativa y un incremento de costos, sino un riesgo indeterminado sobre la interoperatividad global de nuestro modelo.

En tal sentido, adelantamos que en los debates que sobrevengan apoyaremos las posiciones que se orienten a (i) favorecer dicha convergencia global; (ii) simplificar las definiciones de la ley evitando así la posibilidad de interpretaciones contradictorias; (iii) clarificar los roles de las partes intervinientes, en

particular las figuras de encargado y de responsable; y (iv) dada la particular sensibilidad del tema, dar al "tratamiento de datos de niños, niñas y adolescentes" un enfoque integral tomando como principio básico el "interés superior del menor".

Finalmente, entendemos que sería deseable una ampliación del plazo establecido para la presentación de comentarios, dada la complejidad y extensión de la materia en cuestión. Sin perjuicio de ello, manifestamos nuestro interés en colaborar en los pasos futuros de tratamiento del proyecto poniendo a disposición de la Agencia nuestra capacidad de articulación con los sectores representados en nuestra Asociación.

Sin otro particular, la saludamos cordialmente,

Luis Galeazzi
Director Ejecutivo.

:

PROPUESTA PARA LA REFORMA DE LA LEY DE PROTECCION DE DATOS PERSONALES –LEY 25.326-

DRA. AGUSTINA GONZALEZ MIGUENS y DRA. CECILIA NOVOA

Mg. Beatriz Anchorena

Directora de la Agencia de Acceso a la Información Pública

S_____/D_____

De nuestra mayor consideración,

Nos dirigimos a Ud. a los fines de hacerle llegar este documento en el que expondremos tanto los principios como los aspectos sobre los debería estructurarse la nueva ley sobre protección de datos. Sin dejar de lado todos aquellos dilemas o interrogantes sobre los que debería afrontar este proceso de debate a los fines de redactar una ley que resulte eficiente a la hora de interactuar en la sociedad de la información.

Como bien sabemos, el régimen de protección de los datos personales establecido por la ley 25.326-también llamada ley de "hábeas data"- y reglamentado por el decreto 1558/2001, basado en el derecho reconocido por el inc. 3 del artículo 43 de la Constitución Nacional, cuenta con 22 años desde su sanción y un Proyecto de Reforma que, siendo del 2018, quedó obsoleto frente al avance de las tecnologías y de los nuevos modelos de negocio frente a un contexto social, económico y político a nivel mundial atravesado por una pandemia que aceleró sin miramientos el procesamiento de datos que se venían implementando desde principios de siglo.

Al abrirse la mesa de debate impulsada por la Agencia de Acceso a la Información Pública que Usted preside, nos encontramos ante una oportunidad valiosa de poder redactar una ley que se condiga con la realidad que atravesamos, que resulte lo más autosuficiente y protectora de nuestros derechos en cuanto a ser titulares de nuestros datos, posicionando así a la República Argentina como ejemplo de la región.-

Permitir que por cuanto soberanos que somos podamos ejercer un legítimo poder de disposición y control sobre nuestros datos personales, debe resultar ser la piedra angular de nuestra reforma. Destacar que el eje protectorio en el derecho humano fundamental hoy en dia es y debe ser la denominada autodeterminación informativa, la cual nos facultará a decidir cuáles datos queremos proporcionar o no a terceros -sea el Estado o un particular- o qué datos pueden esos terceros recabar, permitiendo asimismo que sepan quién posee nuestros datos personales y para qué, pudiendo inclusive oponerse a esa posesión o uso. Y ese derecho a consentir o no el conocimiento

y tratamiento -informático o no- de los datos personales, requiere como complemento indispensable el consentimiento, que resulta ser el centro del derecho a la protección de los datos personales y muchos de los usuarios carecen de información y hasta concientización de la importancia de sus datos personales.

Entendemos que el planteo de todos estos puntos se haría desde una arista tanto normológica, institucional como técnica:

PLANO NORMOLÓGICO.

La ley 25.326 debería redimensionarse bajo dos aristas: una arista de fondo y otra arista procesal.

Consideramos que bajo el derecho de fondo podrían considerarse los siguientes items:

- Las categorías de datos en la actual ley se analizan en datos personales por un lado y en datos sensibles taxativos por el otro. Opinamos que conforme las características de la sociedad de la información no puede delimitarse el alcance que puede tener tanto los datos como los metadatos sino que debería ser por contexto y/o circunstancias en que se accede a ese dato que delimitaran si el mismo es de acceso público o sensible.
- Las bases de datos tienen que encontrarse registradas y el procedimiento para su registracion debe ser claro, expedito, detallado en sus fines, saber qué datos se recolectarán así como qué medidas de seguridad se tendrán que adoptar frente a la conservación de los mismos. Sin hacer esta tarea ¿cómo sería posible realizar un control por una autoridad de contralor?
- En lo que respecta a la disociación. ¿bajo qué casos tenemos que aplicarla? ¿Para el ámbito judicial solamente? ¿Es viable completamente? ¿Qué sucede con las redes sociales?
- Por lo que corresponde al consentimiento, al margen de ser libre e informado, debería ser expreso, inequívoco y limitado a la finalidad a la que se lo requiere. En el artículo 13 del Anteproyecto del 2022, no se detalla el consentimiento expreso. Nuevamente nos formulamos ¿De qué forma consiente el Titular del Dato el tratamiento de sus datos? Encontramos un vacío legal y en consecuencia la recolección de datos es mediante un "solo aviso" a su titular por el "mero uso".
- Consideramos que se debería analizar la forma en que se recolectan los mails, no puede haber extracción de datos violentando el derecho de información que se da en el ecosistema del derecho de consumo porque a través del harvesting (operación mediante la que se realiza la confección de base de datos de direcciones válidas o en su defecto a través de la compra), nuestro mail

contextualizado en la oferta de bienes y servicios termina siendo extraído y, dentro de un proceso de tratamiento donde se extraen datos que terminan formando bancos y/o registros que en la sociedad de consumo pueden resultar superfluos para ciertos oferentes pero no para otros. De esta manera se generan perfiles que bien pueden ser almacenados o bien vendidos en un ciclo sin fin de acciones que pueden resultar lesivas o cuanto menos intrusivas a nuestra privacidad. Se recomiendan acciones en cuanto a un dato hoy sensible como el mail, el cual termina siendo parte de nuestra identidad. Tengamos presente que el mismo resulta ser trascendental al punto de que hasta en términos judiciales nos sienta notificación sobre diversos actos jurídicos sin contar que es nuestro domicilio virtual ya que nos ubica dentro de una red como es internet. Respecto a esto último, varios son los puntos de debate en cuanto a marcar jurisdicciones y competencias pero serian extenso explicarlos en cuanto a los propósitos de esta previa formalidad al debate aunque sí se sugiere contemplarlos en la reforma como lo han analizado otras normativas.

- A colación con el consentimiento, tampoco se debería admitir condiciones sine qua non para el uso de plataformas, aplicaciones u otros medios´ que se les equipare frente a la negativa de aceptar la recolección de datos que no son a fin a la finalidad de estas.
- La recolección del dato debe realizarse bajo medidas legales justas, transparentes, con propósito claro, limitado únicamente a la finalidad, no excesivo, actualizado y de conservación limitada.
- Con las consecuentes actualizaciones a la política de tratamiento de datos personales deberá solicitarse nuevo consentimiento expreso, en lenguaje claro y detallado.
- Con respecto a los art 14 y 15 del Anteproyecto se plantean mecanismos sencillos, gratuitos y expeditos que tendrá que proveer el responsable del tratamiento de los datos Consideramos que no sólo deberían tenerse en cuenta estas características sino la facilidad de acceso que se le brinda a los titulares de los datos de poder ejercer este derecho de revocación. Se podría analizar la posibilidad de si la autoridad de contralor podría estipular un mecanismo protocolar medular sobre el cual no exista mas dilema al respecto.
- El Art. 18, inc.3 del anteproyecto plantea" *No se podrá realizar el tratamiento de datos personales de menores y adolescentes en los juegos, aplicaciones de Internet u otras actividades que involucren información personal más allá de lo estrictamente necesario para el desarrollo de la actividad.",* refiere a tratamiento como recolección. Se recomienda mas especificidad en lo que respecta a este tipo de recolección de datos.
- Los derechos de los titulares de los datos deben ser GRATUITOS en todo momento, tratándose de información sobre la persona y el derecho inherente que se le atribuye. Además, el responsable del tratamiento es el interesado por

el mismo, debiendo afrontar las cargas administrativas que conlleva el ejercicio del derecho de acceso a la información.

- ¿Qué acción se debería aplicar para un 80% de las PYMES que se encuentran en este país y que no cuentan con la infraestructura y el capital suficiente para sobrellevar acciones que atentan contra sus datos. Deberíamos contemplar un apéndice para los datos de las mismas.
- Como Estado, ¿hacia qué tipo de seguridad aspiramos? Una seguridad por inacción o una seguridad proactiva.
- Instar a la elaboración de una Ley de Cookies, SPAM,y tener intervención técnica a la hora de redactar una ley.

Bajo el plano procesal:

- ¿Sirve un sistema de incremento de multas? ¿O que las empresas queden sujetas a auditorías o procesos de readecuación a la normativa?
- Según el Anteproyecto, en su artículo 20, se plantea: "*En caso de que ocurra un incidente de seguridad de datos personales, el Responsable del tratamiento debe notificarlo a la Autoridad de aplicación dentro de las CUARENTA Y OCHO (48) horas de haber tomado conocimiento, a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos de los Titulares (...)*" Consideramos que dentro de 48 horas e incluso otorgando una extensión del plazo (del cual no se especifica por cuánto tiempo), es poco probable saber efectivamente (aunque no "improbable") si se ha colocado en riesgo los datos de los Titulares. Esto configuraría una vulneración al derecho de acceso a la información hacia el titular del dato. Independientemente que el incidente de seguridad afecte o no al titular del dato, el mismo debería ser notificado. Es decir, el trasfondo sería que nunca se puede saber la ola expansiva de afectación que puede llegar a tener el titular del dato. Si él ejerce su autodeterminación no hay organismo ni estado que lo determine por su persona. Atenta contra su derecho inherente.
- ¿Cuáles son los medios habilitados para realizar denuncias ante la Autoridad de Aplicación? . Deberíamos plantearnos medios factibles, mecanismos de comunicación directos.

PLANO INSTITUCIONAL.

El órgano interviniente en materia de Protección de Datos Personales es la Agencia de Acceso a la Información Pública, vértice del aparato regulatorio a nivel local tanto de la Ley de Acceso a la Información Pública y la Ley de Protección de Datos Personales - Ley

25.326 - y del Registro No Llame. Con la Ley de Acceso a la Información Pública estamos protegiendo un bien jurídico que es la transparencia informativa y el entender que el conocimiento de los actos de gobierno es que nosotros tengamos capacidad de conformar opiniones a su respecto de la manera más acabada posible, lo contrario a privacidad. Todos los principios contenidos en la misma son principios distintos a la de Protección de Datos Personales. El concepto de INFORMACIÓN PÚBLICA y PRIVACIDAD DE DATOS es diferente, siendo así dos ecosistemas diferentes.

- Para fortalecer la responsabilidad en materia de datos en Argentina se necesitará la creación de una autoridad de Control independiente de la Agencia de Acceso a la Información Pública con profesionales versados en la materia para tener un fortalecimiento de la autoridad de control, hacer seguimiento activo en cuestiones de Protección de Datos Personales e instar a las organizaciones y compañías a cumplir con la normativa vigente.
- Que la Agencia de Acceso a la Información Pública constituya la única autoridad de aplicación y control de la Ley de Acceso a la Información Pública –Ley 27.275–
- El Delegado de Protección de Datos Personales deberá contar con "requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones" El Art. 42 del Anteproyecto, no especifica estos requisitos y deberían estar listados los mismos a los fines de un mayor y acabado cumplimiento.

- ¿Deberíamos tener juridictio interregionales? Plantearnos si a nivel nacional, provincial y municipal sería conveniente tener procesos administrativos bajo un sistema de oralidad, utilizando infraestructuras para evitar costos recurriendo en principio a la capacitación y así lograr una mayor expedición.

- Respecto a las fugas, ¿es suficiente la notificación a un organismo de contralor y a los organismos interesados? ¿Evaluamos la velocidad en la que se mueve la técnica con nuestros datos en comparación con el proceso administrativo/judicial actual en donde primero hacemos notificación al organismo? ¿Se mide la magnitud del dato del interesado?

PLANO TÉCNICO

La técnica distribuye el poder que necesita ser equilibrado mediante acciones concretas.

- Contar con personas del ámbito técnico de la seguridad de la información y de la ciberseguridad a la hora de elaborar la presente reforma.
- Hacer hincapié en la tipificación del dato, en qué campo se encuentra sumergido y así poder contar con profesionales abocados en cada materia. No es lo mismo

el manejo de un dato genético como uno bancario.¿ En qué datos el Estado debería intervenir con mayor grado de protección? ¿Qué medidas técnicas viables se pueden implementar para asistir a las organizaciones?

CONCLUSIONES

Es importante subrayar que, por supuesto que resulta más que urgente la necesidad de actualización de la normativa argentina con disposiciones claras sobre estas complejas cuestiones. Desde ya que la creación de una autoridad de control con independencia de la AAIP en lo relativo a Datos Personales, actuando con la debida diligencia, de manera proactiva en sus funciones y controlando que las empresas respeten y cumplan con las normativas vigentes, con profesionales versados en la materia que jueguen a favor de los titulares de los datos, y el mayor conocimiento y capacitación de los usuarios sobre sus derechos dando cabal cumplimiento a la autodeterminación informativa, resultan fundamentales para lograr mayores incentivos en el cumplimiento de la normativa. No debemos resignar nuestra privacidad y protección de datos personales porque nuestra voz vale y como titular del dato tenemos un derecho irrenunciable a nuestra autodeterminación informativa que tenemos que ejercerla. Nuestro bien jurídico que es la privacidad de datos debe ser respetado.

Solicitamos se tengan en consideración estos aportes a los fines de lograr la ansiada actualización de la Ley 25.326 .
Desde ya agradecemos la posibilidad de apertura del debate a los fines de tener una ley actualizada protegiendo así, los derechos de los titulares de sus datos personales.

Saluda a Ud. atentamente,

Dra. Agustina Gonzalez Miguens. T. 130 F. 740 CPACF.
Dra. Cecilia Novoa. T. 136 F. 276 CPACF.

Asociación Argentina TIC,
Video & Conectividad

Ciudad Autónoma de Buenos Aires, 30 de septiembre de 2022.-

Sra. Directora de la Agencia de Acceso a la Información Pública
Sra. Beatriz Anchorena
S / D

Ref.: Resolución N° 119/2022 AAIP
"Anteproyecto de Ley de Protección de Datos Personales"

De mi mayor consideración:

Daniel Oscar Celentano, abogado, Tº 29 Fº 952 (CPACF) con domicilio especial en Avda. de Mayo 749 5º Piso Oficina 31 de la Ciudad Autónoma de Buenos Aires, domicilio electrónico: atvc@atvc.org.ar en representación de la Asociación Argentina TIC, Video & Conectividad (en adelante "ATVC") continuadora de la Asociación Argentina de Televisión por Cable (ATVC) como surge del Poder General Administrativo, Bancario y Judicial que en copia se acompaña y del cual declaro bajo juramento su autenticidad y vigencia tiene el agrado de presentarse ante la Sra. Directora de la Agencia de Acceso a la Información Pública y dice:

I.- OBJETO. -

En el carácter invocado, y siguiendo expresas instrucciones de mi mandante, vengo en legal tiempo y forma a presentar las recomendaciones, opiniones y propuestas respecto de la consulta pública de la referencia.

II.- PRESENTA COMENTARIOS EN GENERAL Y EN PARTICULAR SOBRE EL DOCUMENTO DE CONSULTA. -

Previamente, hago propicia la oportunidad para agradecer a la autoridad convocante la instancia de participación brindada, que permite a todos los sectores involucrados presentar recomendaciones, opiniones y propuestas sobre el tema de referencia.

En ese sentido, y como cuestión preliminar, resulta necesario un profundo análisis económico de las consecuencias de la eventual implementación de un nuevo régimen legal, determinando con claridad cuáles serán las consecuencias de este, tanto para los consumidores como para los actores de la industria, ponderando así, sobre bases concretas, los efectos de la normativa. A tales efectos, resulta recomendable el seguimiento de las "Guidelines" de la OECD para el dictado de regulaciones o considerar la experiencia de Administración de USA (Decretos 12863/93 y 13563/11), las cuales fijan un marco para el dictado de reglamentaciones para todas las agencias de gobierno, requiriendo un informe de costo beneficio de la regulación propuesta.

Sin perjuicio de que en el documento adjunto se efectuarán comentarios correspondientes a cada ítem puesto a consulta, y tratándose de una temática en constante evolución, entendemos que la norma que eventualmente se apruebe debe estar diseñada a fin de procurar una regulación duradera, que cumpla su objetivo no solo procurando el cumplimiento de los principios que derivan de ella por parte de todos quienes se encuentren alcanzados, sino también capacitando y concientizando a la sociedad en general, desde la primera edad, en la importancia de responsabilizarse por el modo y tipo de uso que les dan a sus datos personales, ya que desde allí se crean los más estrictos controles y seguridad, para su tratamiento.

Por otra parte, y a modo de consideración general sugerimos adaptarnos a la normativa existente en la materia tomando ejemplos con el GDPR o la ley de California, evitando plazos más acotados o principios más estrictos o aun no experimentados, como por ejemplo: la definición de datos sensibles, la elaboración de perfiles, la extensión de la minimización de datos, el principio

de exactitud, intentando aprovechar toda su experiencia y camino transitado, evitando por ejemplo consecuencias negativas tales como la “fatiga del consentimiento”.

Por otro lado, debe considerarse que su cumplimiento implicará la realización de importantes inversiones, para empresas de tamaño y facturación de lo más disimiles entre nuestros Asociados, así como sus consiguientes procesos de compra e implementación, por lo cual resulta ineludible la necesidad de reconsiderar su alcance en lo que refiere a las Pequeñas y Medianas Empresas, así como también lo esencial de ampliar su plazo de implementación a 2 años como mínimo, en un esquema gradual que permita a su vez la adaptación a los cambios por parte de los titulares de los datos.

Por último, es imperativo señalar que el Estado en todas sus funciones y jurisdicciones debe cumplir con las mismas obligaciones y deberes que los Responsables del tratamiento de datos, por lo tanto la normativa en análisis no puede permitir de ningún modo que ello no suceda en el ejercicio de sus funciones propias ni justificándose tras ellas.

En lo particular, se especifican nuestras consideraciones puntuales:

Principio de Extraterritorialidad:

Caba mencionar que algunos de nuestros Asociados realizan ofertas de servicio internacionales con el consiguiente tratamiento y/o perfilamiento de datos, ello no solo implica someterse a cada legislación local, (no siempre armónica en esta materia) sino también compatibilizar el cumplimiento de todas ellas y lo que resulta más gravoso aun, generar altísimos costos de operación, lo cual lejos de resultar una ventaja comercial termina convirtiéndose en una eventual barrera de ingreso o permanencia.

Derechos de los titulares:

Consideramos que tanto lo que refiere a los derechos de rectificación, oposición, supresión y autodeterminación informativa, su ejercicio de ningún modo debe atentar contra la libertad de expresión, ni contra la libertad de actividades comerciales ni industriales legitimas, ni del derecho al acceso a la información ni a la continuidad de las prestación de servicio comprometida, ya que ello no solo atenta contra la seguridad jurídica de los Responsables del tratamiento de los datos personales sino también la de los mismos titulares de los datos y su libertad de expresión y elección en general.
En idéntico sentido, es necesario ser muy cuidadoso de los medios y requisitos que se solicitan para el ejercicio de esos derechos, ya que su ejercicio mediante un medio telefónico por ejemplo puede dar lugar exactamente al efecto contrario, vulnerando los principios rectores de la ley. Cuidar a los titulares de los datos, también implica legitimarlos adecuadamente.

Transferencias Internacionales y Evaluaciones de impacto:

En lo que refiere a ambas temáticas, consideramos que la normativa debe fijar los principios esenciales en la materia dando a los titulares las garantías adecuadas para su legítimo desarrollo, sin obstaculizar la actividad de los Responsables obligándolos a someterse a previos controles y aprobaciones.

Incidentes de Seguridad:

Puntualmente, respecto del plazo establecido para la notificación de tales eventos ante la Autoridad consideramos que mínimamente debería ajustarse a la normativa europea en la materia, ello además de definir con mayor claridad y especificidad a que tipo de eventos refiere.

Plazo de Conservación:

En lo que refiere a los plazos de conservación estrictamente necesarios debe tenerse presente el marco regulatorio que regula cada una de las actividades especificas que involucran en el tratamiento de datos, puntualmente en lo que refiere a las telecomunicaciones.

Protección de Datos de Información Crediticia:

Resulta contraria a derecho la inclusión referida a la imposibilidad de tratamiento de datos comerciales negativos referidos a la prestación de los servicios públicos esenciales, ya que atenta contra los Responsables directamente afectados y además podría propiciar, bajo el amparo de la regulación, el ejercicio de una conducta incumplidora en materia de obligaciones de pago.

Régimen Sancionatorio: Multas:

Entendemos que el Régimen Sancionatorio propuesto es excesivamente discrecional y desproporcionado respecto de las facultades que otorga a la Autoridad de Aplicación, en su carácter de Órgano Administrativo, excediéndose sobre actividades por fuera del objeto de la materia objeto de la norma en análisis, nos referimos puntualmente a actuaciones de oficio, clausura de operaciones o suspensión temporal de actividades, la aplicación de medidas correctivas y/o el bloqueo provisional del acceso a la base de datos.

Por otra parte, el monto de las multas propuesto es manifiestamente desproporcionado en referencia a la economía local y peor aun cuando pretende vinculárselo con la facturación global de dicha Compañía, esta es otra oportunidad en la cual, en vez de colaborar con el desarrollo de la economía digital y sus enormes beneficios, una normativa puede resultar inhibitoria de inversiones o desarrollos.

Facultades de la Autoridad de Aplicación:

En lo que refiere al otorgamiento de legitimación activa a la Autoridad de Aplicación para la interposición de acciones colectivas en contra de los Responsables del Tratamiento de datos personales, resulta incompatible con su función de Organismo de Aplicación de la misma ley, dependiente de la Jefatura de Gabinete de Ministros.

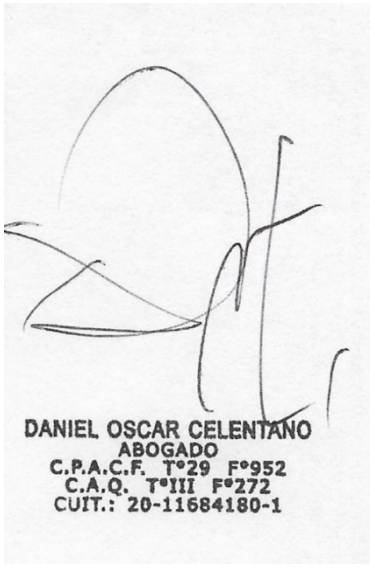
Por otra parte, en lo que refiere a los recursos, el Artículo 56 del anteproyecto es contrario a ley de procedimientos administrativos, afectando el derecho de defensa y la posibilidad de tener una doble instancia. Contradice lo establecido en los art. 94 y 96 del Decreto 1759/72 (Reglamentación de la Ley de Procedimiento Administrativo). La Jefatura de Gabinete es la alzada que aplica (art. 17 de la ley 27.275 actualizada), por lo que sugerimos su modificación.

III.- PETITORIO. -

Por todo lo expuesto, solicito:

1. Se tenga por presentado el escrito en legal tiempo y forma.
2. Se consideren los aportes efectuados por mi mandante.
3. Se tenga presente la reserva del ampliar fundamentos y/o comentarios.

Sin otro particular, saluda a Ud. muy atentamente.



Buenos Aires, 6 de octubre de 2022

Señora Directora de la

Agencia de Acceso a la Información Pública

Mg. Beatriz ANCHORENA

S / D

De nuestra mayor consideración:

Tengo el agrado de dirigirme a Ud. en representación de la Asociación de Empresas de Correo de la República Argentina ("AECA"), en relación al asunto de referencia.

AECA es la cámara empresaria de correos privados líder del sector que opera en la República Argentina. Con casi 20 años de funcionamiento, agrupa a 34 operadores postales que representan casi el 52% del mercado privado en términos de volumen de envíos.

Sus integrantes son los responsables de, entre otras tareas, atender el desafío que implica la distribución de los envíos asociados a operaciones de comercio digital.

En ese rol (que, reiteramos, no agota las múltiples funciones con las que los asociados de AECA contribuyen al comercio y las comunicaciones) hemos observado algunos aspectos del proyecto de modificación de la ley de protección de datos personales que -entendemos- requieren un abordaje específico para cubrir situaciones como las que describiremos más adelante.

Específicamente, debemos destacar nuestro rol de terceros en las operaciones de compraventa *no presenciales*; en ese lugar, los correos tienen desde antaño un rol de custodia de seguridad de los envíos (aun cuando, va de suyo, la obligación al respecto sea de medios y no de resultados).

La modificación por parte de las personas en las formas de adquirir bienes y servicios y la forma en que acceden a ellos, se ha visto alterada desde la aparición y masificación del comercio electrónico, como sistema no presencial y a distancia de compra de bienes y servicios, resultando en este proceso la forma en que cada persona accede al producto un tema esencial en la satisfacción del proceso de compra.

En este contexto, la legislación ha fortalecido desde antaño la protección de los envíos, que están sujetos a secreto por principio constitucional a la vez que se facilita su circulación.

Nuestro rol es relevante, además, para dar certeza a las transacciones. La entrega de los bienes se juzga acreditada o no según las constancias que emitimos con participación de nuestros colaboradores (todos ellos obligados por el secreto postal, porque así lo prevén las regulaciones que obligan, incluso, a la suscripción de declaraciones juradas específicas).

La garantía sobre la ocurrencia de tan importante evento (nos referimos a la entrega, como extremo enormemente significativo de la compraventa) debe dotarse de las seguridades del caso en interés de ambas partes (compradora y vendedora, o remitente y destinatario en la terminología postal).

Es habitual, entonces, que debamos acceder a datos protegidos por normas como aquella puesta a debate a los fines de asegurar la veracidad de los datos de entrega.

No debemos olvidar que el correo resulta ser el operador que tiene por objeto principal cubrir la última milla de entrega de un envío, y que en palabras de la Unión Postal Universal resulta ser el medio idóneo y más calificado para la tarea en tanto constituye el complemento fundamental para llevar a cabo la entrega final y domiciliaria de los envíos que resultan del comercio electrónico.

Está claro que esa cuestión es ajena a la operación económica subyacente y que está sólo abocada a la prestación de un servicio conexo pero independiente a la operación de compraventa que pueden involucrar al remitente, destinatario (y eventualmente, intermediario, ya sea este un portal, sitio, plataforma, etc).

Asociado a esta esencial característica de su objeto, el correo cuenta además con el antecedente de ser custodio de la información a la que accede en la prestación de sus servicios, y que tienen su origen en el principio del secreto postal que no alcanza únicamente a resguardar el contenido desconocido de los envíos que le son confiados, sino los datos de las personas que intervienen en la comunicación, alcanzando en ese menester a los que identifican al remitente y al destinatario. Frente a este cuadro, resulta lógico entender que el prestador postal encargado de la operación de distribución y entrega esté ligado de modo accesorio a la de compra, porque desconoce el contenido y sólo recibe un envío dirigido a un destinatario, y debe asegurar que ese envío sea correctamente entregado.

Es por ello que, en el marco del Anteproyecto de la Ley de Protección de Datos Personales, entendemos que resulta procedente establecer algunas consideraciones sobre el consentimiento para el acceso a ciertos datos personales vinculados a la seguridad de los envíos, para contribuir con ello a la regular presentación de los servicios de correo.

Proponemos a ese organismo que:

a) El artículo 2 de la norma contemple que el consentimiento del titular de datos se entienda dado, también, por su autorización a contratar o por su contratación de servicios conexos a la transacción principal (cuando se trate, obviamente, de operaciones comerciales);

   Esto, aprovechando la definición de *terceros* que porta la norma, pero que no se ve referida de modo significativo en su articulado.

b) El artículo 8 debería recoger previsiones similares;

c) El artículo 12 debería contemplar que las obligaciones legales a que refiere su literal c) incorporen a aquellas emergentes de un contrato como *ley privada*, así como que esos contratos puedan ser principales, conexos o accesorios;

d) El artículo 13 debe reflejar que el consentimiento puede darse por la elección de servicios conexos a una prestación principal. Entendemos que la prestación de servicios postales debe merecer tratamiento específico en el

articulado de la norma, dada la particularidad de estar alcanzada la misma por las normas derivadas del secreto postal como obligación constitucional.

e) El artículo 14 debería prever que la revocación de una autorización puede habilitar la suspensión de las prestaciones pendientes por aquel sujeto que requería de ese permiso para cumplir con sus obligaciones;

f) En general, entendemos que (i) debe preverse la cesión de los datos en el marco de contratos conexos o auxiliares; y (ii) deben morigerarse las multas, contemplándose -además- la situación de los prestadores de servicios de esta naturaleza. A esos fines, estimamos que deberían analogarse respecto de los prestadores postales las normas que limitan responsabilidad por daños o extravíos.

Confiamos en que el temario antes listado podrá enriquecerse tanto con la visión del organismo que Ud. preside como con el devenir del propio análisis de nuestras propuestas.

Aguardamos una respuesta favorable a nuestra solicitud, y aprovechamos esta oportunidad para saludarlo con la más distinguida consideración.

Bárbara Anzini
Apoderada
Asociación de Empresas de Correo
de la República Argentina

ASOCIACIÓN LATINOAMERICANA
DE PRIVACIDAD

Ciudad de Buenos Aires, 11 de octubre de 2022

Sra. Directora

AGENCIA DE LA ACCESO A LA INFORMACIÓN PÚBLICA

Mg. Beatriz de Anchorena

S/D

De nuestra mayor consideración,

Por medio de la presente, le hacemos extensivo un cordial saludo en nombre de la Asociación Latinoamericana de Privacidad (en adelante, ALAP).

ALAP es una organización regional sin fines de lucro que tiene como misión ofrecer un espacio de trabajo colaborativo y capacitación permanente a los profesionales que se encuentran trabajando en protección de datos y privacidad. De esa forma, y como fin último, ALAP busca que la red de profesionales colabore en robustecer un ecosistema en donde la Privacidad y la Protección de los Datos Personales sean pilares para la innovación y el desarrollo sustentable de la región. Todo ello apostando a, de esa forma, potenciar la Economía Digital protegiendo simultáneamente los derechos de las personas.

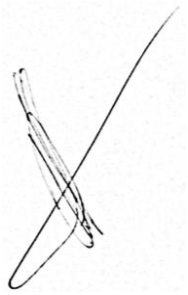
Los miembros asociados a la ALAP son profesionales de la privacidad latinoamericanos que desarrollan sus actividades en diversos ámbitos (público, privado y de la sociedad civil). Su origen latinoamericano no limita el hecho de que actualmente se desempeñen alrededor de todo el mundo.

Es por ello que la ALAP celebra y valora el impulso que la nueva gestión a cargo de la Agencia de Acceso a la Información Pública (AAIP) le ha impreso al Anteproyecto de Reforma de la Ley N°25.326.

En ese sentido, y con el afán de que la nueva norma sea la más adecuada para los fines previamente descritos, le hacemos llegar nuestros comentarios y sugerencias. Ellos surgen a partir de la experiencia que nuestros miembros tienen trabajando día a día en organizaciones de nuestra región, aplicando no solo normas locales sino, en muchos casos, también normas como el Reglamento Europeo de Protección de Datos Personales.

En nombre de ALAP, entonces, agradecemos el proceso de consulta pública que la AAIP está llevando adelante y esperamos que nuestro aporte sea de utilidad para lograr la mejor regulación posible de la materia. Regulación que esperemos modernice nuestra querida Ley N°25.326 y potencie las posibilidades de Argentina de continuar insertándose en la economía global.

Saludamos a Usted cordialmente y quedamos a su disposición.



Dr. Juan Pablo Altmark

Presidente de la Asociación Latinoamericana de Privacidad

Comentarios y sugerencias al Anteproyecto de Ley de Reforma de la Ley 25.326.

Los comentarios y sugerencias se han hecho teniendo en cuenta nuestra actividad profesional, y respecto de los artículos que detallamos a continuación.

1) **ARTÍCULO 1.- Objeto**

En el Anteproyecto se ha mencionado que se garantiza el derecho fundamental de las personas humanas a la protección de sus datos personales y su privacidad, de conformidad a lo establecido en el artículo 43, párrafo tercero, de la Constitución Nacional, los *"los convenios internacionales sobre protección de datos personales y los tratados de derechos humanos en los que la REPÚBLICA ARGENTINA sea parte".*

Consideramos que sería conveniente ampliar el alcance además a aquellos Tratados y Convenciones Internacionales en los que Argentina sea parte y en los que se prevean disposiciones sobre protección de datos personales.

Como ejemplo se puede mencionar el Acuerdo sobre Comercio Electrónico del Mercosur que contiene cláusulas sobre protección de datos personales (desde el artículo cinco en adelante), sin ser un convenio específico sobre la materia.

2) **ARTÍCULO 2°. - Definiciones**

a) Respecto de la definición de ***Datos sensibles****,* sugerimos tener presente que podrían ser innumerables los datos que *"pueden dar origen a discriminación"*. Al dejar abierta la definición, podrían generarse obligaciones concretas como designar un delegado de protección de datos, realizar evaluaciones de impacto o aumentar las medidas de seguridad, entre otras, sobre datos que en principio no lo ameritan pero que, en el futuro, podrían tener un uso potencialmente discriminatorio.

b) Se define ***"Tratamiento de datos"*** como *"cualquier operación o conjunto de operaciones, automatizada, parcialmente automatizada o no automatizada, realizada sobre datos personales, que permita, de manera enunciativa, la recolección, conservación, organización, estructuración, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción y, en general, el procesamiento, así como también su* ***cesión*** *a través de comunicaciones, consultas, interconexiones o transferencias"*.

En este caso sugerimos reemplazar "cesión" por "transmisión", que fue anteriormente utilizado y es de más amplio alcance.

c) Se define a los ***"Datos biométricos"*** como *"aquellos datos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros".*

Consideramos que la mención de las **"imágenes faciales o datos dactiloscópicos"** en este artículo puede generar el entendimiento de que por sí solos son ellos son datos biométricos.

Sin embargo, las imágenes faciales y los datos dactiloscópicos son tipos de datos sobre los cuales, a partir de un tratamiento técnico específico que se realice sobre ellos, pueden surgir el dato biométrico (como patrón o medida estandarizada), pero no son datos biométricos sin llevar a cabo dicho tratamiento.

Por lo mencionado, consideramos conveniente eliminarlos de la definición.

d) Se define al ***"Delegado de protección de datos"*** como *"persona humana o jurídica encargada de informar al Responsable o al Encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos…"*

Al respecto, sugerimos que en lugar de utilizar el verbo informar, se utilice el verbo "asesorar", ya que, si bien son sinónimos, por asesorar se puede entender recomendar, proponer, y consideramos que ello se acerca más a la tarea que tienen los profesionales de privacidad.

Como segunda opción podría mantenerse el verbo "informar" agregando la acción de "asesorar" como sucede luego en el artículo 43 de este Anteproyecto de Ley.

3) **ARTÍCULO 3°. – Ámbito de aplicación material de la Ley**

El citado artículo 3 del Anteproyecto prescribe que *"La presente Ley se aplica al tratamiento de datos personales, incluso cuando los datos personales tratados no formen parte de una base de datos.*

Se deberá conciliar el respeto al derecho a la protección de derechos personales con el derecho a la libertad de expresión. ***En ningún caso se podrá afectar el secreto de las fuentes de información periodística, ni el tratamiento de datos que se realicen en el ejercicio de la libertad de expresión"****.*

Sugerimos en este caso la eliminación de la última oración remarcada en negrita ya que parece contradictorio referirse a la conciliación entre ambos derechos para luego decir que en ningún caso se puede afectar el tratamiento de datos que se realice en el ejercicio de la libertad de expresión.

Libertad de expresión y protección a la intimidad son derechos fundamentales de máximo rango constitucional. Un equilibrio razonable entre uno y otro derecho es elemento sustancial en la democracia.

4) **ARTÍCULO 10º.- Plazo de conservación**

Respecto a la redacción del artículo 10 del Anteproyecto, consideramos que sería importante que se mencionen como excepciones, en el párrafo segundo, tanto el cumplimiento de obligaciones legales como el ejercicio de derechos (por ejemplo, el derecho de defensa en juicio)

5) **ARTÍCULO 15.- Información al Titular de los datos**

El artículo 15 establece que: *"El Responsable del tratamiento debe brindar, antes de la recolección, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, al menos, la siguiente información:*

Inciso a). *"Nombre o razón social, domicilio y medios electrónicos del Responsable o del Encargado. Cuando aplique, del Delegado de protección de datos y, en el caso de los Responsables o Encargados no establecidos en la REPÚBLICA ARGENTINA, los de su Representante en el territorio nacional…"*

Consideramos que esta obligación, tal como surge del Reglamento Europeo, debería ser relativa al Responsable (y no al Encargado).

Inciso e). *"Información sobre posibles cesiones a otros Responsables o Encargados de tratamiento"*

Sobre este punto, en la práctica, podría suceder que la decisión de tercerizar surja mucho después.

Por su parte, en el caso de los Encargados no hay cesión sino transmisión, por lo que tampoco tendría sentido informarlo.

Inciso f) ***"****Información sobre las transferencias internacionales de datos, incluyendo países de destino, identidad y datos de contacto del importador,*

posibles riesgos asociados a las transferencias y salvaguardas aplicables, categorías de datos involucradas, finalidad y mecanismos para ejercer sus derechos".

Aquí sugerimos que en vez de "importador" se hable de información sobre posibles "destinatarios o categorías de destinatarios".

6) **ARTÍCULO 18.- Tratamiento de datos de niñas, niños y adolescentes**

El artículo 18 reza: *"En el tratamiento de datos personales de un menor 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.*

1. Es válido el consentimiento de menor o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información…"

Consideramos que será necesario definir qué se entiende por ***"servicios de la sociedad de la información".***

7) **ARTÍCULO 19.- Principio de seguridad de los datos personales**

El artículo 19 establece que *"El Responsable o Encargado del tratamiento de datos personales deberá sujetarse al principio de seguridad de datos personales, para lo cual adoptara las medidas técnicas, organizativas y de cualquier otra naturaleza que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales…"*

Consideramos que, tratándose de una obligación de medios, no debería exigirse **garantizar la seguridad**.

En tal sentido, sugerimos la siguiente redacción:

*"El Responsable o Encargado del Tratamiento de datos personales deberá sujetarse al principio de seguridad de datos personales, para lo cual adoptar**á** las medidas técnicas, organizativas y de cualquier otra naturaleza que **propendan** a garantizar el acceso, la disponibilidad y la confidencialidad de los datos personales..."*

8) **ARTÍCULO 20.- Notificación de incidentes de seguridad**

Sugerimos llevar el plazo de notificación al plazo establecido en la mayor parte de las normativas que es de 72 horas. No obstante, consideramos que la mejor solución sería que el plazo quede abierto y que sea definido por una resolución de la Autoridad de Aplicación. Esto sería mucho más práctico para darle flexibilidad según evolucione la temática.

Asimismo, consideramos que el primero de los siguientes párrafos es poco claro y redundante con el que le sigue inmediatamente después:

"En caso de no contar con los medios materiales para cumplir el plazo previsto, debe justificar a la Autoridad de aplicación la extensión del mismo".

"Si la notificación a la Autoridad de aplicación no tiene lugar en el plazo previsto, deberá ir acompañada de indicación de los motivos de la dilación".

9) **ARTÍCULO 21.- Deber de confidencialidad**

Respecto a la redacción de la última oración: *"El obligado puede ser relevado del deber de confidencialidad por resolución judicial"*, consideramos que podrían existir otros motivos por los cuales corresponda también relevar del deber de confidencialidad. Por ejemplo, una obligación legal, motivos de seguridad pública, defensa nacional o salud pública, etc.

10) **ARTÍCULO 25.- Excepciones**

Respecto a la redacción de este artículo en cuanto establece que *"…Las excepciones enumeradas en el presente artículo no podrán ser utilizadas para*

realizar transferencias internacionales de forma periódica o habitual, y tampoco cuando involucren a un gran número de personas".

Consideramos que la citada oración final del artículo no debería estar presente ya que es una limitación específica del Reglamento General de Protección de Datos de la UE (GDPR) que está acotada a casos que no cumplen ni con adecuación, ni con garantías, ni son una excepción y tiene requisitos de evaluación más aviso a la autoridad.

11) **ARTÍCULO 26.- Derecho de acceso**

La redacción del artículo 26 sostiene:

Inciso c): *"Los destinatarios o las categorías de destinatarios a los que se* ***cedieron*** *o se prevean ceder los datos personales"*;

Inciso d). *"Información sobre las transferencias internacionales de datos que se hayan efectuado o se prevea efectuar, incluyendo países de destino y* ***base legal que justifica la transferencia****";*

Consideramos conveniente reemplazar los conceptos marcados en negrita por "transmitieron" (para evitar el uso del concepto cesión, que es más acotado) y por "y las garantías adecuadas, en su caso".

12) **ARTÍCULO 27.- Derecho de rectificación**

El artículo en análisis establece que *"El Titular de los datos tiene el derecho a obtener del Responsable del tratamiento la rectificación de sus datos personales, cuando éstos resulten ser inexactos, falsos, errados, incompletos o no se encuentren actualizados.*

En el supuesto de cesión o transferencia internacional de datos erróneos o desactualizados, el Responsable del tratamiento debe notificar la rectificación al cesionario dentro del QUINTO (5°) día hábil de haber tomado conocimiento efectivo del error o la desactualización.

Durante el proceso de verificación y rectificación de la información que se trate, el Responsable debe bloquear el dato, o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión".

Respecto de los términos *"cesión o transferencia internacional"* no queda claro si la cesión debe o no ser internacional

Se menciona al "cesionario" cuando previamente se habla de transferencia, que no necesariamente implica la existencia de un cesionario (por ejemplo, si es dentro de un mismo grupo económico).

13) **ARTÍCULO 28.- Derecho de oposición**

La redacción del artículo en análisis establece que *"El Titular 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".*

Notamos que este párrafo es muy amplio. Deberá interpretarse que el caso de obligación / derecho contractual u obligación / derecho legal son motivos legítimos para el tratamiento, por ejemplo.

"El Titular también puede oponerse al tratamiento de sus datos personales cuando tengan por objeto la publicidad, la prospección comercial o la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con esas finalidades. Cuando el Titular se oponga al tratamiento para esos propósitos, sus datos personales dejarán de ser tratados para dichos fines. El Titular tendrá derecho a que el tratamiento de datos personales se limite

a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el Responsable".

De la redacción de este párrafo surgen algunas inquietudes. Que diga que el Titular "tendrá derecho", implica ¿qué el titular tiene que pedir que se aplique esta limitación?

Ya en el párrafo anterior se establece que *"Durante el proceso de verificación y rectificación de la información que se trate, el Responsable debe bloquear el dato, o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión".*

14) **ARTÍCULO 29.- Derecho de supresión**

El artículo en análisis establece que *"El Titular de los datos tiene derecho a solicitar la supresión de sus datos personales al Responsable del tratamiento.*

La supresión procede cuando:

f. Los datos son tratados para fines de publicidad, prospección comercial o mercadotecnia...".

Consideramos que el literal f) debería completarse con la frase siguiente *"y el titular se hubiera opuesto o retirado el consentimiento"*. En ese caso, igualmente, la situación quedaría cubierta por los literales b) y c).

15) **ARTÍCULO 30.- Decisiones automatizadas y elaboración de perfiles**

El párrafo tercero del artículo en análisis establece que *"El Responsable del tratamiento deberá proporcionar, siempre que se le solicite, información clara, completa y adecuada sobre los criterios y* ***procedimientos*** *utilizados para la decisión automatizada o semiautomatizada, observando secretos comerciales e industriales.*

Consideramos que con la palabra "procedimientos" remarcada en negrita, no parece tener relevancia, y que incluso podría generar conflictos por revelar secretos de negocio.

16) **ARTÍCULO 31.- Derecho a la portabilidad de datos personales**

El artículo 31 sostiene que *“Cuando se traten datos personales mediante medios electrónicos o automatizados, el Titular de los datos tiene derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable o que sean objeto de tratamiento, en un formato que le permita su ulterior utilización o transferirlos a otro Responsable.*

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. Afecte las obligaciones legales del Responsable del tratamiento;

d. Impida que el Responsable del tratamiento proteja sus derechos, seguridad, bienes, o los del Encargado del tratamiento, o del Titular de los datos o de un tercero.

Sin perjuicio de otros derechos del Titular, el derecho a la portabilidad de los datos personales no es procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el Responsable con base en los datos personales del Titular”.

Respecto a la redacción de este artículo, notamos en este punto que, a diferencia del Reglamento General de Protección de Datos, este derecho no se ha limitado a los datos tratados en base legal en el consentimiento y cuando sean necesarios para la ejecución de un contrato. Entendemos que de esta forma los Responsables quedan desprotegidos respecto a los datos que hayan inferido luego de un análisis y evaluación propia, que no tiene por qué beneficiar a otro responsable.

En todo caso, el nuevo responsable tendrá que, con los mismos datos personales, hacer su propio análisis.

17) **ARTÍCULO 32.- Ejercicio de los derechos**

Sugerimos ampliar el plazo para que el Responsable dé respuesta al Titular de los Datos y/o permitir que se solicite una prórroga en caso de que corresponda. El plazo de 10 días que establece el Anteproyecto resulta exiguo, teniendo en cuenta la experiencia de la actual Ley N°25.326 que prevé plazos similares. Además, sugerimos contar el plazo desde que el titular del dato ha brindado toda la información necesaria para acreditar su identidad, en caso en que no lo haya hecho al pretender ejercer el derecho.

18) **ARTÍCULO 33.- Excepciones al ejercicio de los derechos**

Entendemos que no tiene aplicación práctica que la ley establezca condiciones sobre leyes posteriores (respecto a cuál debería ser su contenido) que, por esa condición, derogaría a la Ley que se está proponiendo.

19) **ARTÍCULO 34. Deberes del Responsable del tratamiento**

En el literal d) se hace referencia a las “medidas de seguridad necesarias”. Consideramos conveniente describirlas como **“medidas de seguridad adecuadas”**.

Respecto al literal m), éste parece establecer como obligatoria la designación de un Delegado de Protección de Datos sin dejar abierta la posibilidad de que en el futuro la AAIP pueda reglamentar si será o no obligatorio en todos los casos (para lo cual se podrían utilizar diferentes criterios como facturación, cantidad de empleados, categoría de datos, etc.).

20) **ARTÍCULO 35.- Encargado de tratamiento**

En relación con la redacción del literal e), ¿Puede la autoridad realizar auditorías? ¿Qué diferencia tiene con las inspecciones? En todo caso, tiene sentido que la Autoridad verifique el cumplimiento de la ley, pero no del contrato, salvo que afecte la privacidad de los titulares, en cuyo caso actuaría verificando el cumplimiento de la ley.

Respecto al Literal j), podría suceder que las solicitudes presentadas por el Titular no puedan o deban ser respondidas por el Encargado, salvo que el Responsable así lo haya indicado y por lo tanto se considere ello parte del servicio que presta el Encargado.

En el literal h), se establece que el Encargado deberá "*Tratar los datos personales bajo condiciones de* ***seguridad necesarias*** *para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".*

Entendemos que sería más acertado, a nuestro criterio, hablar de medidas de seguridad "adecuadas".

El literal k), menciona la necesidad de informar a la Autoridad de aplicación y al Responsable las "*violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares*". Parecería que se está hablando de notificación de incidentes de seguridad. Al igual que en el artículo 34 literal h), sugerimos aclarar si realmente se trata de incidentes de seguridad.

Por otra parte, consideramos que es erróneo imponer esta obligación sobre el Encargado. El Reglamento Europeo no lo ha hecho y entendemos que ello busca evitar diversos inconvenientes:

1- La multiplicación de notificaciones a la Autoridad de Control. Recordemos que incluso pueden existir sub Encargados que, entonces, deberían notificar a la Autoridad y al Encargado, que a su vez debería notificar a la Autoridad y al Responsable, que a su vez debería notificar a la Autoridad (esto por no dar un ejemplo aún más extremo).

2- La notificación del Encargado a la Autoridad sería previa a la notificación del propio Responsable, ya que el plazo para este último comenzaría a correr desde ese momento de la notificación (a ambos). Así, las notificaciones a la Autoridad sobre un mismo incidente serían seguramente diferentes, ya que contando con más días el Responsable podría contar con más información y detalle.

En definitiva, sobre esta obligación, no logramos observar la ventaja para el Titular del dato. El Responsable tiene el deber de exigir que el Encargado lo notifique y, luego, en ciertos casos, notificar a la Autoridad de control.

Esta innovación entendemos que solo traería dificultades en la relación cada vez más frecuente entre Responsables y Encargados (y los potenciales sub procesadores).

En el literal l), al igual que en el caso del Responsable, no precisan criterios para la designación del delegado de protección de datos.

21) **ARTÍCULO 36.- Política de tratamiento de datos personales**

Respecto a este punto nos llama poderosamente la atención la exigencia de que la Política conste en un medio físico además de en medio electrónico.

Asimismo, que se exija una nueva autorización en caso de haber cambios sustanciales, cuando no siempre será necesario el consentimiento o autorización para poder tratar los datos personales de los Titulares.

22) **ARTÍCULO 38.- Protección de datos desde el diseño y por defecto**

El artículo en análisis establece que *“El Responsable del tratamiento y el Encargado deben, desde el diseño y antes del tratamiento, prever y aplicar medidas tecnológicas y organizativas apropiadas para cumplir los principios y garantizar los derechos de los Titulares de los datos establecidos en la presente Ley.*

Las medidas deben ser adoptadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de los datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus Titulares.

El Responsable y el Encargado del tratamiento deben aplicar las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, sólo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplica a la cantidad, calidad y categoría de datos personales tratados, al alcance de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas deben garantizar que, por defecto, los datos personales no sean accesibles, sin la intervención del Titular de los datos, a un número indeterminado de personas humanas".

Respecto de la redacción de este artículo, consideramos que:

a) Esta obligación no podría imponérsele a los Encargados de Tratamiento ya que ellos no son quienes determinan los fines y medios del tratamiento.

b) Por otra parte, consideramos necesario aclarar que la protección de datos desde el diseño y por defecto no se aplica solo antes del tratamiento, sino que ello también debe ser revisado durante el todo el tratamiento.

c) Respecto de los riesgos que entraña el tratamiento, ellos no solo podrían afectar el derecho a la Protección de Datos, sino que también otros derechos podrían ser afectados, por lo que sugerimos no especificar.

23) **ARTÍCULO 39.- Evaluación de impacto relativa a la protección de datos personales**

El artículo en análisis sostiene que deberá realizarse Evaluación de Impacto en PDP cuando haya *"b. Tratamiento de datos sensibles a gran escala, de datos relativos a antecedentes penales, contravencionales o de niños, niñas y adolescentes"*

Consideramos que si el Código Civil y Comercial permite que los adolescentes puedan brindar su consentimiento para ciertos actos y establece su autonomía progresiva, parecería contradictorio suponer que esos casos, y solo esos, tienen un riesgo mayor.

24) **ARTÍCULO 41.- Informe previo**

En su redacción, el artículo 41 sostiene que *"Cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo, el Responsable debe informar a la Autoridad de aplicación".*

Entendemos que vale la pena aclarar que el alto riesgo debe subsistir luego de la aplicación de las acciones de mitigación.

25) **ARTÍCULO 42.- Delegado de protección de datos**

La redacción del artículo en análisis establece que *"…El Responsable del tratamiento estará obligado a respaldar al Delegado de protección de datos personales en el desempeño de sus funciones…"*

Sin mayores comentarios sobre lo desarrollado en este artículo, solamente hacemos mención que al momento de hacer hincapié al respaldo al Delegado de protección de datos, no se ha mencionado, a diferencia de lo que sucede en el resto del artículo, al Encargado de tratamiento.

26) **ARTÍCULO 43.- Funciones del delegado de protección de datos**

El literal g) del artículo 43 sostiene que es función del DPD *"Recibir las comunicaciones y responder los reclamos de los Titulares"*.

Sobre el literal g, queremos destacar que la carga de responder los reclamos, o mejor dicho al ejercicio de derechos de los titulares de los datos, recae sobre el Responsable o, eventualmente, sobre el Encargado (si a ello se ha comprometido) y **no sobre el Delegado de protección de datos que tiene por función**, **como el mismo artículo lo menciona, solamente asesorar al respecto.**

27) **ARTÍCULO 44.- Representantes de Responsables y Encargados del tratamiento no establecidos en la República Argentina**

Sobre este artículo consideramos que se trata de un error convertir a un punto de contacto en un garante.

Entendemos que limitará absolutamente las posibilidades de organizaciones locales de brindar ese tipo de servicios y, al mismo tiempo, también las de las organizaciones establecidas fuera de Argentina de ofrecer sus productos y servicios en nuestro país.

Si la finalidad del artículo es lograr la responsabilidad del Responsable o Encargado no establecido en la Argentina, consideramos que existen mecanismos de cooperación suficientes para ello.

En caso de mantenerse esta obligación, consideramos que debería hablarse de "garante" en vez de "representante".

28) **ARTÍCULO 51.- Facultades de la Autoridad de aplicación**

En su redacción, el artículo en análisis establece que es facultad de la Autoridad de Aplicación *"…d. Solicitar información a los Responsables o Encargados de tratamiento, Delegados de protección de datos y Representantes, los que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de datos que se le requieran; en estos casos, la Autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;"*

Respecto a la facultad de solicitar información, consideramos que no debiera mencionarse a los Delegados y a los Representantes. Ellos podrán ser puntos de contacto, pero la información debe solicitarse a los Responsables y Encargados ya que quienes tienen el deber de informar son estos últimos.

29) **ARTÍCULO 58.- Sanciones**

En su redacción el artículo sostiene que "*…En todos los casos la Autoridad de aplicación dará a publicidad la resolución en su sitio web y, si lo considere pertinente, en el Boletín Oficial y ordenará su publicación en el sitio web del Responsable, a su costa".*

Sobre la publicación en BO y en sitio web del Responsable consideramos que, más allá de la consideración de la pertinencia y que se hace referencia a la futura reglamentación del artículo, debería atarse esta posibilidad a algún parámetro de criticidad del caso.

30) **ARTÍCULO 60.- Multas**

El monto de las multas, de más de 66 millones de dólares, parece desproporcionado comparando con las demás regulaciones del mundo.

Es tal la desproporción que, pese a que no tiene impacto directo en el ejercicio profesional de los Delegados, nos hace temer que pueda ser un obstáculo para el fluido avance del Anteproyecto en los pasos que quedan para llegar a ser ley.

31) **ARTÍCULO 75.- Derogación**

El artículo en análisis establece que *"Con la entrada en vigencia de la presente Ley, quedan derogadas las Leyes Nros. 25.326 y 26.343, con excepción de lo dispuesto en el artículo 32 de la Ley 25.326 texto ordenado por Ley N.º 26.388".*

Notamos aquí un posible vacío legal ya que la ley entra en vigencia al ser publicada, pero hay un año para su implementación, tiempo durante el cual, según este artículo, la Ley N°25.326 estaría derogada. Consideramos que sería conveniente mantener el enfoque del Proyecto anterior, con entrada en vigencia dentro de un año, pero mientras tanto manteniendo la vigencia de la Ley N°25.326, al menos en deberes y derechos, y sanciones.

Buenos Aires, 11 de octubre de 2022

Sres.
Agencia de Acceso a la Información Pública
Atn.: Mg. Beatriz Anchorena

Ref.: Anteproyecto de Ley de Protección de Datos Personales
Agencia de Acceso a la Información Pública (AAIP)

De nuestra mayor consideración:

En atención al vencimiento del plazo para la consulta sobre el anteproyecto de la referencia Por la presente, se acercan los comentarios ampliados a la propuesta de anteproyecto de Ley de Protección de Datos Personales.

A continuación, se exponen los comentarios y conclusiones jurídicas con relación a cada uno de los artículos específicamente citados:

1. ART. 2 DEL PROYECTO. DEFINICIÓN DE DATOS SENSIBLES:

✓ **Texto del Proyecto de Ley de la AAIP:**

"*Aquellos que se refieran a la* ***esfera íntima*** *de su Titular,* ***o cuya utilización indebida puedan dar origen a discriminación*** *o* ***conlleve un riesgo grave*** *para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical u opiniones políticas; datos relativos a la salud, discapacidad, a la preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona humana*".

✓ **Comentario**:

Se considera que la definición genérica o enunciativa produce inseguridad jurídica, y resulta más conveniente el criterio de la ley actual que es también compartido por el *"Reglamento General de Protección de Datos"* (RGPD)[1], donde se menciona en concreto qué es un dato sensible prescindiendo de una definición.

Debe destacarse que la vulneración de la normativa resulta en la imposición de sanciones de multa, razón por la cual la clara definición de la norma es fundamental en virtud del principio de legalidad, y la prohibición de analogía.

[1] El Reglamento General de Protección de Datos (RGPD) es el marco regulatorio comunitario dedicado a la protección de datos y a la privacidad relativo a todas las personas y empresas dentro del territorio de la Unión Europea (UE). Entró en vigor el 25 de mayo de 2016 y pasó a ser de obligado cumplimiento dos años después: el mismo día de 2018.

2. ARTS. 2 Y 20 DEL PROYECTO. NOTIFICACIÓN DE INCIDENTE DE SEGURIDAD:

✓ **Texto del Proyecto de Ley de la AAIP:**

(i) Define al incidente de seguridad de datos personales como la ocurrencia de uno o varios eventos en cualquier fase del tratamiento que atenten contra la confidencialidad, la integridad y la disponibilidad de los datos personales.

(ii) Prevé que, en caso de que ocurra un incidente, el responsable del tratamiento debe notificarlo a la Autoridad de Aplicación dentro de las 48 horas de haber tomado conocimiento, **a menos que sea improbable que dicho incidente de seguridad constituya un riesgo para los derechos de los Titulares de los datos**. De igual manera, prevé que el responsable del tratamiento también debe informar al Titular de los datos sobre el incidente de seguridad ocurrido, en un lenguaje claro y sencillo, cuando sea probable que **entrañe altos riesgos a sus derechos**.

✓ **Comentarios**:

(i) Se entiende que no resulta necesario ni conveniente tener una definición de incidente de seguridad, pues, podría ocurrir que exista un incidente de datos en los términos definidos pero que no suponga ningún peligro real e inminente para los titulares ni para el responsable. El RGPD, norma por excelencia que regula la materia, no tiene definición de este concepto, sino que exige la notificación al regulador y a los usuarios "*en caso de violación de la seguridad de los datos personales*…".

(ii) Se considera que se podría mejorar el texto de la norma evitando el calificativo de "altos" riesgos, pues, se podría malinterpretar y resulta ambiguo. Se recomienda utilizar un texto más similar al del RGPD que expone, directamente, la necesidad de notificar cuando se vislumbre un "*un riesgo para los derechos y las libertades de las personas*…".

(iii) Se agrega que RGPD contempla el plazo de 72hs para notificar un incidente de seguridad. "*En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente… sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella…"* (art 33 RGPD).

(iv) En este sentido, siguiendo la línea del RGPD, se sugiere que el plazo dispuesto para la notificación de un incidente de seguridad pase a ser de setenta y dos (72) horas de haber tomado conocimiento, a diferencia de las cuarenta y ocho (48) horas que prevé el proyecto de reforma.

Por otra parte, la forma en que está estructurado este artículo podría tender a confundir la notificación dirigida a la autoridad de aplicación con la que corresponde al titular de los datos. En ese sentido, consideramos que podría ser útil que el último párrafo del artículo *("El Responsable del tratamiento debe…")* pase a ser el segundo, siguiendo al primer párrafo que finaliza de la siguiente manera: "*deberá ir acompañada de indicación de los motivos de la dilación"*.

Asimismo, atendiendo a lo que sucede en la práctica y la imposibilidad de recolectar la información requerida sobre un incidente de seguridad en un plazo tan corto, se considera que este artículo debería prever en forma clara y específica que el informe dirigido a la autoridad de aplicación es independiente del aviso de haber tomado conocimiento del "incidente". En ese sentido, parece correcto mantener el criterio de que la información requerida sea enviada, sin dilación alguna, a medida que sea posible.

3. ARTS. 22 A 24 DEL PROYECTO. TRANSFERENCIAS INTERNACIONALES (CAP. 3).

✓ **Comentarios**:

Se solicita tener en cuenta el texto del RGPD en el sentido de *permitir expresamente el intercambio de datos entre entidades que conforman un mismo grupo económico*. (v.gr.: art 47 RGPD Normas corporativas vinculantes).

4. ART. 25 DEL PROYECTO. EXCEPCIONES

✓ **Texto del Proyecto de Ley de la AAIP. Primer párrafo:**

"Las transferencias internacionales podrán realizarse excepcionalmente si se cumplen algunas de las siguientes condiciones (…)".

✓ **Comentario**:

Se considera que debería mejorarse el texto citado con la modificación resaltada: "Las transferencias internacionales podrán realizarse excepcionalmente si se cumple ***al menos UNA (1)*** de las siguientes condiciones".

5. ART. 30 DEL PROYECTO. DECISIÓN AUTOMATIZADA O SEMIAUTOMATIZADA:

✓ **Texto del Proyecto de Ley de la AAIP:**

(i) Se regula que el titular de los datos tiene derecho a no ser objeto de una decisión basada única o parcialmente en el tratamiento automatizado de datos, que le produzca efectos jurídicos perniciosos, lo afecte significativamente de forma negativa o tenga efectos discriminatorios.

(ii) Se prevé que, en caso de que, debido a secretos comerciales e industriales, no el Responsable no pueda brindar información sobre los criterios y procedimientos utilizados para la decisión automatizada o semiautomatizada la AAIP podrá realizar auditorías en el tratamiento automatizado o semiautomatizado.

✓ **Comentarios:**

(i) El primer párrafo que incorpora un texto similar al contenido en el al RGPD con relación a las decisiones basadas en el tratamiento automatizado de datos, pero con

importantes modificaciones, debería reconsiderarse. Su inclusión, con la redacción pretendida, afecta el delicado equilibrio que debe existir entre el derecho personal y la evolución natural de la tecnología. La mera automatización no resulta un perjuicio y la normativa debe tender a prevenir este último y no meros hechos objetivos.

(ii) En línea con lo anterior, se considera que deberían contemplarse excepciones que admitan per se el uso de tratamiento automatizados, como lo hace el RGPD para los casos de celebración o ejecución de contratos y el consentimiento explícito del interesado.

(iii) Asimismo, se considera excesivo que se abarque el caso de procesamientos parciales automatizados.

(iv) Se entiende que la facultad de realizar auditorías sobre secretos comerciales e industriales resulta contraria a la ley de propiedad intelectual e industrial, y deriva en una potestad excesiva por parte del regulador. Dicha facultad no está contemplada en el RGPD, lo cual es una buena medida de comparación.

6. ART. 44 DEL PROYECTO. REPRESENTANTES DE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO NO ESTABLECIDOS EN LA REPÚBLICA ARGENTINA:

✓ **Texto del Proyecto de Ley de la AAIP:**

(i) Esta figura aplicable cuando el Responsable o el Encargado del tratamiento no se encuentren establecidos en ARGENTINA y un registro de inscripción.

✓ **Comentario:**

Se considera que esta incorporación implica un pesado requisito formal que conspirará con iniciativas de procesamiento en el exterior, además de la creación de un registro como carga burocrática. Muchos proveedores del exterior no podrán o perderían interés en prestar servicios en la Argentina en función de tener que cumplir con este requisito.

7. ART. 49 DEL PROYECTO. DEBER DE COMUNICACIÓN. ANÁLISIS CREDITICIO:

✓ **Texto del Proyecto de Ley de la AAIP:**

(i) Para los supuestos en que los Responsables de tratamiento elaboren un sistema de puntuación y/o calificación de acuerdo con el comportamiento crediticio de las personas, 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.

✓ **Comentario:**

En línea con el análisis efectuado, no resulta razonable exigir que el Responsable del tratamiento comparta esta información que implica secretos comerciales. La utilización de estadísticas, algoritmos, variables y cálculos no es materia propia de los "datos personales" sino que hace a la libertad de comerciar y ejercer una industria lícita, conforme al art. 14 de la C.N.

8. ART. 60 DEL PROYECTO. SANCIONES. MULTA:

✓ **Texto del Proyecto de Ley de la AAIP:**

(i) Se estipulan multas con unidades de medida que van desde 5 hasta un 1.000.000; o, del dos por ciento (2 %) hasta el cuatro por ciento (4 %) de la facturación total anual global del ejercicio financiero anterior.

✓ **Comentarios:**

(i) No resulta razonable que haya dos criterios, entendiéndose que, como en otras legislaciones, el criterio fijo en todo caso debe ser el tope para el porcentual.

(ii) Se considera excesiva y exorbitante la pretensión de establecer una multa sobre la base de la facturación global. Debe señalarse que el antecedente de la UE en el caso no resulta aplicable en tanto dicha normativa es dictada en el ámbito de una Unión Económica. En el caso de la Argentina la vinculación a facturación a nivel global pierde toda razonabilidad y proporcionalidad de la sanción pretendida. La normativa debería copiar el sistema legislativo de Brasil que prevé multas sobre la facturación para todo el conglomerado corporativo de un grupo económico, pero dentro del país y no a nivel global.

9. ART 68 DEL PROYECTO. TRÁMITE:

✓ **Texto del Proyecto de Ley de la AAIP. Segundo párrafo:**

"*El plazo para contestar el* ***informe*** *no podrá ser mayor a CINCO (5) días hábiles, el que podrá ser ampliado prudencialmente por el juez*".

✓ **Comentario:**

Se considera que se puede mejorar la redacción del segundo párrafo modificando la palabra "informe" por "requerimiento", teniendo en cuenta que lo que se le instruye al responsable no es la contestación de un informe, sino justamente la remisión de la información del accionante.

10. ART 70 DEL PROYECTO. AMPLIACIÓN DE LA DEMANDA:

✓ **Texto del Proyecto de Ley de la AAIP. Segundo párrafo:**

"*Contestado el informe, el actor podrá, en el término de* ***TRES (3) días****, ampliar el objeto de la demanda, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por igual término para que conteste y ofrezca prueba*".

✓ **Comentario:**

En línea con los distintos artículos del texto del proyecto, y a fin de evitar confusiones, sugerimos que se aclare que el plazo estipulado es de tres (3) días **hábiles**.

***

Esperando vuestra respuesta favorable a las peticiones formuladas y a las consideraciones preliminares efectuadas, saludamos muy Atte.

Paz Adrogué
Asesora de Presidencia
Asociación de Bancos de la Argentina

ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES

Aportes y observaciones de la Asociación del Personal Legislativo (APL)

El desarrollo y la innovación de la ciencia aplicada a la tecnología, especialmente en los progresos que se fueron dando en este siglo, han tenido un profundo impacto en todos los ámbitos de las relaciones interpersonales, lo que hizo posible cambios cada vez más veloces en los escenarios actuales y en las perspectivas futuras.

La actividad laboral no escapa a esta lógica. El trabajo en su visión tradicional ha sido objeto de decisivos procesos de transformación, que fueron creando nuevos paradigmas y oportunidades, pero también nuevos desafíos. Las herramientas y los insumos imprescindibles para llevar a cabo las tareas laborales en estos tiempos requieren de adecuados conocimientos, normas y protocolos que garanticen su buen uso.

La era digital y de la información promovió una revolución de los modelos de la comunicación. A su vez, trajo consigo una extrema vulnerabilidad en la seguridad, en la privacidad y en la intimidad de las personas. Creemos que es imprescindible brindar un marco de protección estatal que sea compatible con una visión actual del problema y acompañe los procesos de desarrollo tecnológico en un entorno seguro.

Celebramos la iniciativa promovida por la Agencia de Acceso a la Información Pública, con la convicción de que una nueva ley de protección de datos personales permitirá dar respuesta los desafíos que plantean los usos de las nuevas tecnologías, particularmente en lo referido a las relaciones laborales y al ejercicio de los derechos de los trabajadores y las trabajadoras.

El presente documento se elabora con el fin de ser presentado dentro del proceso de debate participativo, abierto y transparente para la actualización de la Ley 25.326 de protección de Datos Personales.

A tal fin enumeramos las propuestas que a nuestro criterio deben ser tenidas en consideración para alcanzar una legislación en la materia que defienda los derechos laborales de las personas. En síntesis:

1. Los derechos fundamentales de los trabajadores y las trabajadoras en la actualidad se ven atravesados por la recolección, el almacenamiento y tratamiento de datos de carácter personal dentro de la relación de trabajo. Por tal motivo debería considerarse y regularse de modo diferenciado a la protección de datos personales del trabajador y la trabajadora en su calidad de sujeto social hipervulnerable.

2. En esa inteligencia debería reconocerse expresamente el derecho a la autodeterminación informativa de los trabajadores y las trabajadoras. Actualmente la libertad informática en el trabajo y la consecuente protección de sus datos es condición sine qua non para la operatividad de todo el sistema jurídico vigente en materia laboral.

3. El consentimiento expreso, libre, informado, inequívoco y específico debería ser establecido como la base fundamental y excluyente para la legitimación de cualquier tipo de tratamiento de datos personales. En el particular, en consonancia con derecho comparado, como excepción a esta regla mínima se podría considerar la creación de ficheros de datos por parte del empleador únicamente con la finalidad de verificar el cumplimiento de los deberes y obligaciones laborales de los trabajadores y las trabajadoras. Sin embargo, como contracara resulta imperioso disponer que la prescindibilidad de consentimiento previo del trabajador, como requisito legitimante para el procesamiento de sus datos a estos fines, no exceptúa al empleador del deber de notificar a sus empleados, previamente y de modo expreso e inequívoco, sobre la existencia de un fichero o tratamiento de datos de carácter personal, del objetivo de la recolección de éstos y de los posibles destinatarios de la información resultante. Así como también de las consecuencias de la obtención de estos datos, o de la negativa a brindarlos, y la posibilidad de ejercer los conocidos derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)

4. Bajo este entendimiento se debería disponer que el empleador: a) Debe notificar fehacientemente a los trabajadores sobre la finalidad del procesamiento de sus datos b) No está autorizado a recolectar más datos de los estrictamente necesarios a los fines declarados c)

No está legitimado a utilizar los datos de sus trabajadores y trabajadoras con una finalidad distinta del control que le corresponde a su calidad de empleador.

5. Ante el procesamiento de datos biométricos por empleadores mediante sistemas de reconocimiento facial, y atento a la naturaleza sensible de esos datos, se debería hacer especial hincapié en el resguardo de esos datos con medidas de protección y seguridad reforzadas, en la limitación estricta del uso de los datos de acuerdo con la finalidad para la cual son obtenidos, en proporcionarle a los empleados y empleadas toda información relativa al tratamiento de sus datos mediante estas técnicas, así como dónde se almacena, quiénes acceden a esa información, etc. El uso de controles de acceso a las instalaciones a través de la aplicación de datos biométricos, la instalación de sistemas de videovigilancia, el registro de la jornada laboral y/o salarios, así como el uso de sistemas de geolocalización de los trabajadores y las trabajadoras son cuestiones delicadas que ameritan un análisis y regulación pormenorizado donde se dispongan medidas de control y responsabilidades detalladas para el tratamiento, el almacenamiento y la eliminación de los datos que generen.

6. Ante la ocurrencia de un incidente de seguridad que produzca una brecha de datos personales de empleados públicos o privados, debería extenderse la obligación de notificar tal suceso a la asociación sindical que agrupa a los trabajadores afectados por la filtración.

7. Debería también reconocerse específicamente a las asociaciones sindicales la posibilidad de ejercer la representación de los trabajadores y las trabajadoras cuyos derechos hayan sido afectados por incumplimientos de los deberes de quienes fueran empleadores responsables del tratamiento de sus datos, o por la omisión a la hora de efectivizar el ejercicio de alguno de los derechos de los titulares, peticionando ante la autoridad administrativa competente y en sede judicial, otorgando expresamente legitimación activa a la asociación sindical para el inicio de acción de Habeas Data cuando se trate de afectación de datos correspondientes a los trabajadores y trabajadoras que ésta represente.

8. En el marco de una relación laboral desarrollada mediante la modalidad de trabajo a distancia (también conocida como

"teletrabajo"), se debería informar específicamente al trabajador o la trabajadora cuáles son los datos adicionales que se tratarán, observando los principios de proporcionalidad y de limitación de la finalidad, así como contar con una base legítima que permita demostrar que ante una evaluación de ponderación ese tratamiento extra está justificado.

9. Deben realizarse capacitaciones periódicas y obligatorias en el tratamiento de datos personales a quienes intervienen en todo el proceso de obtención, almacenamiento, conservación, organización, transferencia y evaluación, etc.

10. Respecto a representantes de responsables, quienes tengan a su cargo el tratamiento de datos personales no establecidos en la República Argentina y de las personas autorizadas para el tratamiento de datos, debe expresamente disponerse la responsabilidad solidaria de estos, habilitando al o la titular de datos personales, su representante legal u asociación sindical a exigir indistintamente de manera individual o en conjunto el cumplimiento de los derechos y obligaciones dispuestos en la presente ley.

Norberto Di Próspero

Secretario General

Asociación del Personal Legislativo

Matías D'Onofrio, presidente de la Comisión de Ciencia y Tecnología de APL, Dr. Lucas Barreiro, Dra Laura Lissi, Dr. Franco Endrek, Dr. Ignacio Perillo.

Ciudad de Buenos Aires, 11 de octubre de 2022

Mg. Beatriz de Anchorena
Directora
Agencia de Acceso a la Información Pública
S / D

Ref: Procedimiento de Elaboración Participativa de Normas - Propuesta anteproyecto actualización Ley N° 25.326 - RESOL-2022-119-APN-AAIP

De nuestra mayor consideración:

Luis Galeazzi, titular del Documento de Identidad N° 11.427.841, en mi carácter de Director Ejecutivo de **ARGENCON**, constituyendo domicilio en Talcahuano 833, Piso 10 Of. A, C1013AAQ, Ciudad Autónoma de Buenos Aires, Argentina, en el marco del Procedimiento de Elaboración Participativa de Normas, conforme lo establecido en el Reglamento General aprobado por el artículo 3° del Decreto Nº 1172/03 (Anexo V), nos dirigimos a Uds. a fin de presentar nuestros comentarios con relación a la propuesta de Anteproyecto de Ley de Protección de Datos Personales (IF-2022-94737490-APN-AAIP) (el "Anteproyecto").

I. ARGENCON

ARGENCON es la primera entidad del país que nuclea a empresas prestadoras de servicios de todos los verticales de la Economía del Conocimiento (https://www.argencon.org/institucional/). Nucleamos a las empresas del conocimiento con orientación exportadora y liderazgo en sus rubros de actuación. Actualmente, nuestra comunidad de socios está conformada por 45 empresas líderes que integran seis clústeres: Centros de Servicios Globales, Servicios Profesionales, Biotecnología, Empresas de IT, Medios y Tecnología Productiva. La Economía del Conocimiento exporta hoy un valor superior a U$S 7,2 mil millones anuales, y ocupa más del 7% del empleo registrado en el país. Nuestros asociados representaron en 2021 más del 25% del total de las exportaciones nacionales.

Trabajamos para generar las condiciones que favorezcan el desarrollo del sector y la formación de talento digital, además de promover el crecimiento de las exportaciones y el posicionamiento de Argentina como líder en la prestación de servicios del conocimiento a nivel global. En distintas actividades que configuran la Economía del Conocimiento el tratamiento de datos es intensivo y constituye la esencia del mundo digital. Por tal motivo valoramos muy positivamente la invitación a sumar nuestra opinión al debate que se inicia para actualizar la Ley N°25.326 de Protección de Datos Personales mediante el aporte de las sugerencias que se consignan a continuación, ello con el objetivo de facilitar los usos beneficiosos e innovadores de los datos en un entorno de negocios y tecnológico en constante evolución, lo cual en última instancia garantizará la competitividad económica del país.

II. COMENTARIOS AL ANTEPROYECTO

A continuación, se detallan una serie de comentarios con relación a determinados artículos del Anteproyecto, siguiendo su numeración:

(i) **Artículo 2. Definiciones**. En lo que refiere a la definición de "*datos sensibles*" y "*datos biométricos*", consideramos que:

- Es preferible recurrir a la técnica legislativa de la Ley De Protección de Datos Personales No. 25.326 en la cual se lista de forma taxativa qué categorías de datos comprende la definición de dato sensible. De esta manera, se evitaría caer en subjetividades en la interpretación de lo que puede entenderse como *"que pueda dar origen a discriminación*", cerrándose así la puerta a ambigüedades y arbitrariedades en su aplicación.

- Debe eliminarse de su definición al dato biométrico, ya que, de acuerdo con su actual definición propuesta en el Anteproyecto, se incluyen las imágenes faciales, lo que desdibujaría el propósito de protección reforzada que busca el Anteproyecto. Recordamos, siguiendo la línea del Reglamento Europeo de Protección de Datos Personales, en su considerando 51, que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de datos sensibles, ya que únicamente deben encontrarse comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. En consecuencia, sugerimos modificar también la definición de datos biométrico quitando la referencia a las "imágenes faciales" o aclarando lo antedicho.

(ii) **Artículo 4. Ámbito de aplicación territorial.** En relación con el inciso a) del presente artículo, consideramos que:

- Es sugerible clarificar si bajo el mismo, la ley resultará aplicable a Responsables o Encargados que se encuentren en Argentina, pero realicen tratamiento de datos personales de individuos que no se encuentren en Argentina.

- Si fuese de la manera prevista en el numeral precedente, no resultará de fácil cumplimiento por parte de los Responsables o Encargados quienes no solo deberán cumplir con las legislaciones en materia de protección de datos personales del país de residencia o domicilio del titular del dato, sino también con la legislación argentina por el sólo hecho de estar situado en el país. Esto podría dar lugar a contradicciones en las obligaciones previstas en las normativas que deberían cumplir en razón de este artículo.

(iii) **Artículo 12. Bases legales para el tratamiento de datos.** En lo que hace a la base legal relativa al interés legítimo del Responsable del tratamiento y la evaluación detallada que se deberá realizar, consideramos que:

- Dicha evaluación, tal como se encuentra prevista, puede resultar en un análisis subjetivo que escapa los deberes de posible cumplimiento a cargo del Responsable.

- Sería conveniente limitar, basado en lo anterior, el alcance de la evaluación de forma tal que el Responsable pueda realizarla de manera objetiva, por ejemplo, considerando fórmulas como *"incluyendo el contexto y las circunstancias en las que se llevará a cabo el tratamiento, utilizando criterios de proporcionalidad y razonabilidad".*

- Sugerimos definir cuál será el criterio de la evaluación y qué debe realizarse con las conclusiones arribadas. Entendemos que, en línea con el Reglamento Europeo de Protección de Datos Personales, la evaluación implica documentar cuál es el interés legítimo *vis-a-vis* el tratamiento del dato en particular.

(iv) Artículo 13. Consentimiento.

- En relación con la definición de consentimiento (artículo 2), allí se señala que el consentimiento debe ser expreso, libre, inequívoco, informado y específico. Pareciera que la definición encuentra una contradicción con el artículo 13 del Anteproyecto que determina que el consentimiento debe ser previo, libre, *específico*, informado e inequívoco. Es decir, el artículo 2 requiere que el consentimiento sea expreso, mientras que el artículo 13 no. Esto genera una contradicción en los requisitos para la recolección del consentimiento que debería de ser resuelta toda vez que "inequívoco" y "expreso" constituyen dos fórmulas diferentes para el tratamiento de datos personales, por lo que consideramos que no es posible que ambos requisitos concurran como acumulativos. Destacamos que el estándar internacional es que el consentimiento sea inequívoco para el tratamiento de datos personales y que solo deba ser expreso para el tratamiento de ciertas categorías especiales de datos.

- La exigencia de obtener consentimientos específicos para cada finalidad del tratamiento posiblemente pueda generar en los Responsables la necesidad de dejar de usarlo como base legal y de recurrir a las otras fórmulas previstas en el Artículo 12 del Anteproyecto, perdiendo en la práctica una fuente legitimadora del tratamiento que resulta conveniente y adecuada en diversas ocasiones.

- La obligación impuesta en el artículo 13 (*in fine*) relativa a la carga de evidenciar por parte del Responsable que el Titular consintió el tratamiento de sus datos personales, por fuera del consentimiento informado otorgado a tal efecto, puede resultar en varias ocasiones de cumplimiento imposible o, por lo menos, muy dificultoso.

(v) **Artículo 22 y 24. Transferencias internacionales.**

- Se permiten las transferencias internacionales cuando el exportador de los datos ofrezca garantías apropiadas. El Anteproyecto no define ni brinda mayor información sobre el concepto de "*garantías apropiadas para el tratamiento*". Una lectura holística de sus artículos sugiere que estas garantías podrían ser las enumeradas en el artículo 24. Sin embargo, la redacción actual podría ser considerada ambigua en sus términos. Sugerimos realizar la aclaración pertinente.

- El Anteproyecto pone en cabeza del exportador la carga de probar que la transferencia internacional es realizada conforme a lo dispuesto por la ley. Sobre esto último, el Anteproyecto pareciera poner esta carga independientemente del rol. Es decir, que quien se ocupe de transferir los datos internacionalmente, sea este el Encargado o el Responsable, debe responder frente a la Autoridad de Protección de Datos por el mismo. Esto podría generar el escenario en el que, por ejemplo, el Encargado que se ocupa de recolectar los datos personales en Argentina y transferirlos al Responsable en el extranjero, sea quien deba demostrar que la transferencia internacional fue realizada conforme lo dispuesto por la ley, a pesar de que el Responsable era quien instruyó dicha transferencia. Por lo tanto, sería sugerible contar con mayores aclaraciones al respecto.

- Al igual que en la Ley de Protección de Datos Personales No. 25,326 y normas complementarias (es decir, las Disposiciones N° 60-E/2016 y N° 159/2018), el Anteproyecto establece que pueden surgir niveles adecuados de protección, entre otros, de (a) cláusulas contractuales modelo aprobadas por la Autoridad de Protección de Datos o (b) normas corporativas vinculantes aprobadas por la Autoridad de Protección de Datos. No resulta claro aún si las disposiciones ya emitidas por la Autoridad de Protección de Datos seguirán vigentes si y cuando se apruebe el Anteproyecto y, por lo tanto, tampoco resulta claro si las cláusulas

contractuales estándar actuales y las pautas para las normas corporativas vinculantes serán reemplazadas o no.

- Adicionalmente, mientras que la Disposición 60-E/2016 de la Autoridad de Control de Protección de Datos establece que tanto el exportador como el importador están sujetos a su jurisdicción, el Anteproyecto establece que el acuerdo o mecanismo implementado para la transferencia internacional de datos personales debe garantizar que el importador esté sujeto a la jurisdicción de una o más autoridades de control independientes para que los Titulares de los Datos tengan acciones legales efectivas para ejercer sus derechos. No resulta claro aún si el hecho de estar sujeto a una autoridad extranjera independiente se considerará suficiente para que el importador de datos cumpla con este requisito.

- Por último, en su redacción actual, el consentimiento del titular del dato o el cumplimiento de un contrato, sólo pueden utilizarse para las transferencias internacionales de datos personales con carácter excepcional y, por tanto, no pueden utilizarse para las transferencias internacionales realizadas de forma periódica o habitual, y tampoco cuando involucren a un gran número de personas. Este punto resulta importante ya que es una práctica común en las actividades de los miembros de ARGENCON, limitándose así las herramientas que se poseen para poder realizar las transferencias.

(vi) **Artículo 30. Decisiones automatizadas y elaboración de perfiles.**

- Sugerimos eliminar toda referencia a la decisión basada “parcialmente” o “semi” automatizada, en tanto las mismas ya implican la existencia de intervención humana.

- Para evitar subjetividades, sugerimos eliminar la mención a la “discriminación” y reemplazarlo por “*efectos jurídicos perniciosos o lo afecte significativamente de forma negativa”*

(vii) **Artículo 35. Encargado de tratamiento.** Recomendamos:

- Clarificar cuál será el contenido mínimo que debe incluir el contrato que deberá celebrarse entre los Responsables y Encargados conforme el inciso a., por ejemplo, indicando si es aquel incluido en el inciso f. del presente artículo (contratos entre encargados y sub-encargados).

- Clarificar a qué se refiere que el subcontratado asumirá la calidad de Responsable ante el incumplimiento de sus obligaciones y responsabilidades.

- Especificar a qué se refiere con “*tramitar*” las solicitudes presentadas por el Titular de los datos. No es claro si el Encargado debe responderlas por obligación legal. Si ese fuera el caso, detectamos una imposibilidad práctica para poder darle curso a dicha obligación por una gran cantidad de Encargados. De acuerdo a lo establecido por las buenas prácticas en el mundo solo los Responsables reciben los requerimientos de los Titulares ya que son quienes interactúan directamente con los Titulares, teniendo en cuenta la naturaleza del tratamiento y la información disponible para el Responsable.

- Limitar el plazo en el cual Encargado pueda ser auditado por parte del Responsable a una vez por año.

- Limitar la notificación de "*violaciones de seguridad*" al Responsable y quitar la referencia del inciso .k sobre informar al Responsable y a la Autoridad de Control sobre "violaciones a códigos de seguridad". A la vez, no resulta claro si se refiere a Incidentes de Seguridad o a la violación de cualquier política interna de seguridad del responsable.

- Clarificar si la "*persona o área que asuma la función de protección de datos* personales" es equivalente al delegado de protección de datos o si es una figura diferente. En caso que lo sea, sugerimos definirla en el artículo 2 del anteproyecto.

(viii) **Artículo 39. Evaluación de impacto relativa a la protección de datos personales.**

- Sería conveniente definir qué es lo que se considera como "*tratamiento de datos sensibles a gran escala*" o "*evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado o semi-automatizado*" como factor que hace aplicable la obligatoriedad de realizar la evaluación de impacto. A la vez, sugerimos limitar la exigencia de realización de evaluaciones de impacto únicamente respecto de los tratamientos automatizados (y no semiautomatizados) en los que se basen las evaluaciones sistemáticas y exhaustivas de aspectos personales de las personas humanas.

- Por último, no queda claro si continuará vigente la "Guía de Evaluación de Impacto en la *Protección* de Datos" (https://www.argentina.gob.ar/sites/default/files/guia_final.pdf).

(ix) Artículo 41. Informe previo.

- Sugerimos adoptar medidas de responsabilidad proactiva si se detecta un alto riesgo para los derechos de los titulares de los datos, toda vez que importaría una carga desmedida para la Autoridad de Aplicación tener que aprobar los informes finales de las evaluaciones de impacto. De la misma manera, importaría un perjuicio desmedido para los Responsables el no poder iniciar los tratamientos hasta tanto no se tenga la autorización de la autoridad de aplicación.

(x) Artículo 60

- Sugerimos aclarar el significado de "facturación global" en el artículo 60 como la facturación de la entidad (persona jurídica) infractora, independiente de si integra un grupo económico, ello a fin de garantizar que las multas sean proporcionales.

Finalmente, manifestamos nuestro interés en colaborar en los pasos futuros de tratamiento del proyecto poniendo a disposición de la Agencia nuestra capacidad de articulación con los sectores representados en nuestra Asociación.

Sin otro particular, la saludamos cordialmente,

Luis Galeazzi
Director Ejecutivo.

ADEPA

Buenos Aires, 11 de octubre de 2022

Señora
Lic. Beatriz Anchorena
Directora
Agencia de Acceso a la Información Pública (AAIP)

Su Despacho

Me dirijo a Usted en relación con la consulta pública sobre la propuesta de actualización de la Ley 25.326, de Protección de Datos Personales, para hacerle llegar una serie de comentarios en nombre de la Asociación de Entidades Periodísticas Argentinas (ADEPA).

Comparto a continuación los comentarios:

La necesidad de contemplar a la actividad periodística como un caso especial dentro del ejercicio de la libertad de expresión y diferenciarla de las grandes plataformas de internet.

La libertad de expresión es un derecho esencial e insustituible para la realización de todo ser humano. Nadie puede ser dignamente concebido sin la libertad de expresar su pensamiento. Al mismo tiempo, este derecho constituye un insumo o condición necesaria e indispensable para la vigencia del sistema democrático, ya que hace posible la participación de la ciudadanía en la discusión y toma de decisiones sobre asuntos de interés público.

Desde esa perspectiva, la libertad de expresión se encuentra garantizada a toda persona por el solo hecho de serlo. Y, como lo expresó la Corte Interamericana de Derechos Humanos, no debe ser restringida a un grupo de individuos o a una determinada profesión[1]. Sin embargo, ciertos grupos de personas, como es el caso de quienes ejercen el periodismo, debido al relevante papel que desempeñan en la sociedad a través del ejercicio de su derecho a la libertad de expresión, son objeto de una atención y tutela especiales. Así es como los Estados "tienen la obligación de adoptar medidas especiales de prevención y protección de los periodistas sometidos a un riesgo especial por el ejercicio de su profesión"[2].

[1] Cfr. Cor.I.D.H., Caso Tristán Donoso v. Panamá, 27.01.2009, *párr.* 114.
[2] Cfr. Cor.I.D.H., Caso Vélez Restrepo y Familiares v. Colombia, 3.09.2012, *párr. 194*.

Al mismo tiempo, el periodismo no es solo una profesión individual. La misma Corte Interamericana ha destacado, en hora reciente, que "los medios de comunicación social juegan un rol esencial como vehículos para el ejercicio de la dimensión social de la libertad de expresión en una sociedad democrática, razón por la cual es indispensable que recojan las más diversas informaciones y opiniones… '[s]on los medios de comunicación social los que sirven para materializar el ejercicio de la libertad de expresión, de tal modo que sus condiciones de funcionamiento deben adecuarse a los requerimientos de esa libertad"[3].

Precisamente en esa misma sentencia se advirtió que "para que la prensa pueda desarrollar su rol de control periodístico, debe no solo ser libre de impartir informaciones e ideas de interés público, sino que también debe ser libre para reunir, recolectar y evaluar esas informaciones e ideas". Y agregó en el mismo lugar el tribunal que "el Relator especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de las Naciones Unidas se refirió a que las personas que desarrollan una actividad periodística 'observan, describen, documentan y analizan los acontecimientos y documentan y analizan declaraciones, políticas y cualquier propuesta que pueda afectar a la sociedad, con el propósito de sistematizar esa información y reunir hechos y análisis para informar a los sectores de la sociedad o a esta en su conjunto'" [4]. Así es como concluye que "cualquier medida que interfiera con las actividades periodísticas de personas que están cumpliendo con su función obstruirá inevitablemente con el derecho a la libertad de expresión en sus dimensiones individual y colectiva"[5].

Desde esta perspectiva, en tanto la labor del periodismo supone la búsqueda, recolección y análisis de información que, en muchos casos, es información personal (i.e. "datos personales"), en ocasiones información sensible (i.e. "datos sensibles"), la aplicación de la legislación de datos personales constituiría una traba evidente al ejercicio de la profesión y, por ende, al interés social que explica también la preocupación por asegurar la libre circulación de información.

La propuesta de anteproyecto, en su artículo 3, admite que "se deberá conciliar el respeto al derecho a la protección de derechos personales con el derecho a la libertad de expresión" y agrega, de inmediato, que "[e]n ningún caso podrá afectar el secreto de las fuentes de información periodística, ni el tratamiento de datos que se realicen en el ejercicio de la libertad de expresión".

En consonancia con lo anterior, se considera necesario, a fin de evitar cualquier tipo de ambigüedad, aclarar que la aplicación de la ley "en ningún caso podrá afectar el secreto de las fuentes de información periodística, ni el tratamiento de datos que se realice en el ejercicio de la libertad de expresión *o de la actividad periodística*".

---

[3] Cor.I.D.H., Caso Moya Chacón v. Costa Rica, 23.05.2022, *párr.* 66.
[4] *Ibidem*, *párr*. 67. Subrayado añadido.
[5] *Id. ant*.

Con esto se procura dejar en claro que la ley deja afuera de su ámbito de aplicación todo el tratamiento de datos que realiza la empresa periodística como tal, al menos en tanto se vincule en forma directa a las fuentes de información, los archivos periodísticos, la relación con los lectores y la audiencia, por mencionar algunos ejemplos.

A su vez, y con la finalidad de que el principio expuesto en el artículo 3 del proyecto se mantenga incólume, corresponde aclarar en el artículo 13: "*En ningún caso el consentimiento del titular de los datos será requerido para la recolección o el tratamiento de los datos cuando esa actividad tenga por finalidad el ejercicio y desarrollo de la actividad periodística. Esa posibilidad no protege la comisión de ilícitos para acceder al dato*".

El periodismo tiene por finalidad reconstruir la realidad a partir de los datos y de la información a la cual logra acceder a través de investigaciones y fuentes de distinta naturaleza. En tanto esos mecanismos de recolección de información no supongan la comisión de un acto ilícito por parte del periodista, el consentimiento del titular de esos datos para su incorporación a la actividad periodística constituye un obstáculo insalvable al ejercicio del periodismo.

Esta libertad en la recolección de la información no debe confundirse con la impunidad para su posterior publicación. La publicación de esa información por parte del periodismo será lícita o ilícita de acuerdo con los estándares constitucionales que protegen la libertad de expresión, la intimidad y el honor ("Campillay", "real malicia", etc.). Pero la decisión de publicar cierta información solo puede tener lugar una vez que se acceda a esos datos; por ello es que el consentimiento como barrera a la recolección de información personal por parte de la empresa periodística afecta los aspectos más elementales de su labor.

Del mismo modo, las autoridades no deberían imponer exigencias que supongan interferir o desalentar la difusión de información y/o su acceso a través del acceso a los sitios de internet de los medios periodísticos. Con ese fin, se propone aclarar algo que se encuentra implícito en el artículo 3, incorporando como párrafo final al artículo 15 el siguiente texto: "*En ningún caso se podrán imponer exigencias técnicas que limiten la libre navegación por los sitios de internet de los sitios periodísticos*".

Si bien lo indicado en los apartados anteriores es suficiente –y determinante– para excluir a periodistas y empresas periodísticas del ámbito de aplicación de una reforma a la Ley de Protección de Datos Personales, es importante tener presente también las grandes diferencias que existen entre la prensa y otras empresas que, incluso cuando ejerzan distintos aspectos vinculados con la libertad de expresión, no pueden ser consideradas empresas periodísticas ni puestas en un pie de igualdad con ellas.

Nos estamos refiriendo a las grandes plataformas tecnológicas, las cuales, si bien permiten y facilitan el acceso a información, son en realidad grandes herramientas para la recolección y tratamiento de datos personales con el fin de utilizarlos luego con fines económicos, publicitarios y de toda otra índole.

El principio constitucional de igualdad recogido en los artículos 16, 75 y ccds. CN no solo exige la creación de categorías razonables, sino que también veda, en términos generales, la posibilidad de unificar las consecuencias normativas para situaciones que en la realidad son distintas. Ello es así pues desde el punto de vista constitucional, hacer prevalecer el principio de igualdad supone reconocer que, en ciertas circunstancias, puede ser tan injusto imponer la misma solución a quienes están en desigual situación como tratar en distinta forma a quienes se encuentran en una misma situación[6].

Esta última regla constitucional se vería flagrantemente transgredida si los medios de prensa fuesen colocados en un lugar similar al de grandes plataformas tecnológicas transnacionales.

Atentamente,

Daniel Dessein, presidente

Asociación de Entidades Periodísticas Argentinas
Chacabuco 314, 3º piso. (1069) Ciudad de Buenos Aires. (011) 4331-1500.
adepa@adepa.org.ar . www.adepa.org.ar . Twitter: @adepargentina

[6] Fallos 343:1688, voto jueces Maqueda y Rosatti.

ITI Promoting Innovation Worldwide

Respuesta del ITI a la consulta pública de Argentina para actualizar la Ley de Protección de Datos Personales

11 de octubre de 2022

Mag. Beatriz de Anchorena
Directora
Agencia de Accesso a la Información Pública

Gracias por darnos la oportunidad de comentar acerca del proyecto de ley de Protección de Datos Personales que la Agencia de Acceso a la Información Pública (AAIP) proporcionó al público el 12 de septiembre de 2022.

El Consejo Industrial de Tecnología de la Información (*Information Technology Industry Council*, ITI) es el defensor principal mundial de la tecnología y representa a las empresas más innovadoras. Fundado en 1916, el ITI es una asociación de comercio internacional que tiene un equipo de profesionales en cuatro continentes. Fomentamos políticas públicas y normas industriales que potencian la competencia y la innovación en el mundo. Nuestros miembros y personal experto diversos proveen a los legisladores la perspectiva más amplia y expertos en las áreas de tecnología, *hardware*, *software*, servicios e industrias relacionadas.

La privacidad, la seguridad y la confianza son centrales para las operaciones globales de nuestras filiales, y nuestras empresas tienen interacciones directas con los regímenes de protección de datos y de privacidad de casi todos los países. Con la información de nuestra perspectiva global y experiencia amplia, el ITI incentiva a los gobiernos a desarrollar marcos normativos y legislativos para proteger la información personal y usarla de manera responsable, incentivar la innovación, promover el crecimiento del comercio y facilitar el flujo libre de información. Tenemos el agrado de contribuir a la AAIP ya que considera las actualizaciones sobre la legislación de protección de datos.

Los enfoques interoperables globalmente son esenciales para apoyar la innovación, la creación de puestos de trabajo y el crecimiento económico en la era digital. Elogiamos el reconocimiento de la AAIP de la necesidad de modernizar el régimen actual de protección de datos. También nos gustaría incentivar a la AAIP a considerar cómo se pueden acercar todos los interesados, incluidas las autoridades

públicas, las fuerzas del orden, los intelectuales, las instituciones de investigación y la industria, para reflexionar sobre las funciones que cumplen la protección de la privacidad y los flujos libres de datos para respaldar la economía global. Para ese objetivo, motivamos a la AAIP a intentar lograr una mayor participación de los interesados antes de presentar la legislación en el Congreso para considerar las respuestas sustanciales de aquellos que quizá no tengan la posibilidad de presentar sus comentarios antes de la fecha de entrega o que quisieran agregar comentarios de apoyo.

Por lo tanto, presentamos con el debido respeto al gobierno de Argentina las recomendaciones a continuación que reflejan la posibilidad de desarrollar mecanismos robustos e interoperables de manera global para proteger la privacidad de los datos personales y la seguridad de las personas y para mantener una adecuación con la Unión Europea (UE). Esperamos intercambiar estas ideas y estamos a su disposición para continuar el debate.

Recomendaciones generales

La certeza jurídica y las definiciones claras son fundamentales para la implementación exitosa de todo marco jurídico y más aun en el contexto de un marco basado en riesgos. Aunque la ley ya incluye ciertas definiciones para guiar la aplicación de la ley misma, algunas definiciones jurídicas aún no son claras y dan lugar a interpretaciones diferentes que pueden no ser coherentes con la interpretación integral de la ley, como con la transferencia internacional de datos, el derecho a oponerse y el interés legítimo. El ITI incentiva a la AAIP a definir con claridad los conceptos en la legislación y a considerar desarrollar ejemplos para apoyar más la implementación y el cumplimiento correcto de la ley.

Interoperabilidad de los mecanismos de transferencias de datos entre países

El flujo libre de datos es fundamental para la solidez de la economía moderna global y la disponibilidad de servicios para los usuarios en todo el mundo. Proporciona un sinnúmero de beneficios, que incluyen el crecimiento económico y la innovación, y permite a personas de todo el mundo acceder al conocimiento y las herramientas. Las trasferencias de datos entre países y la protección de la privacidad significativa no se deben percibir como excluyentes mutuamente ni como objetivos antagonistas. En muchas ocasiones, las transferencias entre países son el fundamento para que las organizaciones garanticen los niveles más altos de seguridad de datos para los usuarios en cualquier parte del mundo. Elogiamos la atención que pone Argentina en estos problemas actualmente y solicitamos que el anteproyecto de ley conserve múltiples enfoques que mantienen el salvoconducto de la privacidad para las transferencias de datos entre países.

Es crucial que toda normativa sobre transferencias de datos entre países se alinee con los enfoques internacionales viables que predominan y que cubren todas las

situaciones como entre responsables del tratamiento, de responsable a encargado del tratamiento, de encargado a responsable del tratamiento y entre encargados del tratamiento. Garantizar la coherencia con la protección de datos y los marcos de privacidad adoptados por los socios comerciales reduce la posibilidad de obstáculos en la transferencia de datos personales que realizan las empresas desde Argentina a otras jurisdicciones y viceversa, lo que permite a los usuarios de Argentina continuar gozando del acceso a los productos y servicios. Por ello, aconsejamos a los legisladores intentar lograr una mayor interoperabilidad entre los sistemas jurídicos y las herramientas de transferencia para garantizar el flujo sin interrupciones de datos a nivel global y para evitar suspensiones infundadas o innecesarias de transferencias de datos que puedan impactar tanto a las organizaciones como a los ciudadanos.

Recomendamos que la AAIP modifique el artículo 24.1 (c) del anteproyecto de ley para reconocer los acuerdos contractuales existentes y los instrumentos de transferencia internacional que se alinean con las protecciones que son lo suficientemente similares y sustanciales a aquellas requeridas por la ley de Argentina y las contienen. Por ejemplo, si una empresa ya usa un contrato que se basa en las Cláusulas Contractuales Tipo de la UE, ese instrumento contractual puede contener protecciones sustanciales similares a las que requiere la ley argentina, y por lo tanto no se debería requerir que la empresa celebre un nuevo contrato que contenga las mismas protecciones. Este enfoque fomentaría la interoperabilidad y aumentaría la eficiencia a la vez que mantendría el nivel alto de protección de datos que requiere la ley argentina.

Además, el ITI recomienda que Argentina intente lograr la participación en el foro de las Normas de Privacidad Internacional (*Cross-Border Privacy Rules*, CBPR) global que se expondrá según las CBPR de APEC y que se creó recientemente para apoyar la interoperabilidad y la estandarización de los enfoques reguladores sobre la protección de datos y la privacidad. Australia, Canadá, Singapur, Japón, Estados Unidos, la República de Corea, Taiwán y las Filipinas ya son parte de esta iniciativa.

Asimismo, el ITI anima a la AAIP a que continúe reconociendo las Normas Corporativas Vinculantes (*Binding Corporate Rules*, BCR) y a que negocie el reconocimiento mutuo de las BCR con otras autoridades de protección de datos para garantizar que todo esquema desarrollado para empresas argentinas alcance los beneficios de la transferencia de datos entre jurisdicciones. De manera alternativa, se incentiva que desarrolle un proceso que permita y facilite la evaluación de una aprobación futura de las BCR autorizadas por otras autoridades de protección de datos.

Definición de transferencia internacional de datos

El anteproyecto de ley define la transferencia internacional de datos como toda transferencia de datos personales fuera del territorio nacional. Esta definición es amplia, y el ITI sugiere que se modifique la definición para que quede claro que los

datos enviados directamente por un titular de datos (interesado) a un responsable o un encargado del tratamiento ubicados fuera del país no es una transferencia internacional de datos a los fines de la aplicación del capítulo 3 del anteproyecto de ley (Transferencias internacionales). En particular, recomendamos que se limite la definición para que solo se aplique cuando los datos se transfieran de una persona jurídica a otra persona jurídica en otra jurisdicción. Debido a cómo se creó y se desarrolló la internet global, los datos viajan de forma física entre países como parte de casi todas las actividades en línea, incluso si la actividad se realiza de forma nacional en su totalidad y no hay cambios en el responsable ni en el encargado del tratamiento de datos. En otras palabras, los datos se pueden transferir de la parte A a la B, ambas ubicadas en Argentina, pero fluyen por fuera de Argentina al transferirse de A a B. Esto significa que los datos se mueven técnicamente entre países, pero se aplican las mismas leyes y políticas. La internet se creó como un popurrí descentralizado de decenas de miles de redes diferentes que se conectan y comunican entre sí. Cada una de estas redes dirige datos alrededor del mundo. Las normativas que rigen esas transferencias amenazan con romper las redes y conexiones que son necesarias para que internet funcione.

Por ejemplo, el Comité Europeo de Protección de Datos (CEPD) ha emitido recientemente directrices que incluyen referencias a los tres elementos acumulativos que deben estar presentes para que se pueda definir una transferencia internacional de datos personales[1]. Según estas directrices, una transferencia de datos es una transferencia internacional cuando “1) un responsable o encargado del tratamiento de datos está sujeto al Reglamento General de Protección de Datos (RGPD) para el tratamiento dado; 2) un responsable o encargado (“exportador”) divulga mediante transmisión o hace que de otro modo queden disponibles los datos personales, de este tratamiento, a otro responsable, corresponsable o encargado (“importador”) y 3) el importador se encuentra en un país tercero o es una organización internacional, indistintamente de que este importador esté sujeto al RGPD con respecto al tratamiento dado en conformidad con el artículo 3”. Este enfoque provee los elementos que deben estar presentes para caracterizar transferencias internacionales de datos.

El ITI también recomienda a la AAIP que elimine la última oración del artículo 25 y que aclare el artículo 25 (b), ya que el anteproyecto actual no es claro. Según este, la última oración del artículo 25 establece que las excepciones para transferencias internacionales de datos no se aplican a transferencias realizadas “de forma periódica o habitual, y tampoco cuando involucren a un gran número de personas”. Su eliminación garantizaría que las empresas que dependen de los flujos de datos entre países para ofrecer sus productos y servicios puedan operar en Argentina.

El artículo 25 (b) también debería aclararse para apoyar la transferencia de datos

[1] Consulte las Directrices 05/2021 del CEPD sobre la interacción entre la aplicación del artículo 3 y las disposiciones de transferencias internacionales según el capítulo V del RGPD. Página 4: https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

personales para el cumplimiento de un contrato con el titular de datos (interesado), para realizar las etapas previas al contrato según solicitud del titular de datos o como parte esencial de la provisión de un servicio solicitado por el titular de datos, incluido el reclutamiento y la gestión de empleados. En ese caso, la transferencia mencionada debería realizarse sin que se necesiten más herramientas o mecanismos de transferencia (por ejemplo, una aprobación de la autoridad).

La clarificación mencionada apoya la libertad de dirigir una empresa y refleja que, a veces, las obligaciones contractuales sobre los titulares de datos incluyen transferencias regulares de datos personales y un número significativo de titulares de datos en contextos como de comercio electrónico, empresas emergentes, comunicaciones y viajes.

Además, es importante resaltar que la capacidad de depender de esta exención no exime a la organización del cumplimiento con el principio de responsabilidad según se establece en el artículo 22 del anteproyecto de ley.

Consentimiento

El consentimiento es un mecanismo importante para ayudar a equilibrar los derechos de las personas para controlar sus datos personales y los de derechos de las organizaciones que recopilan, tratan y transfieren datos personales con fines legítimos. Sin embargo, advertimos sobre los requisitos prescriptivos y detallados acerca de la naturaleza y el momento oportuno del consentimiento. Para que el consentimiento sea eficaz, debe ser acorde al contexto. Dado que la naturaleza del tratamiento de datos está en constante evolución, los regímenes de privacidad deberían permitir métodos y técnicas de solicitud de consentimiento para evolucionar al mismo ritmo, mientras se mantiene el control del usuario sobre a quién confía el tratamiento de sus datos personales.

La definición actual de consentimiento en el artículo 2 es muy estricta y podría ser poco práctica para los titulares de datos y las empresas si se aplica de una manera que no sea coherente con la UE y otras jurisdicciones. El consentimiento busca darles a los titulares de datos el poder de tomar decisiones informadas sobre si permiten el uso de sus datos y cómo lo permiten, en especial en el entorno sin conexión. Sin embargo, la exigencia de una acción clara e innegablemente afirmativa del titular para cada tratamiento podría resultar molesto, impactar en la innovación y posiblemente generar más confusión para los usuarios. La AAIP debería esforzarse para proveer un enfoque flexible que sea sensible a la realidad en la que se obtiene el consentimiento en la práctica, que sea muy dependiente del tipo de actividad o del método con el que se recopila, como así también del contexto general de su uso.

Fundamentos legítimos para el tratamiento de datos

Nos agrada que la AAIP reconozca múltiples fundamentos para el tratamiento de datos personales. Esto se coincide con las legislaciones adoptadas a nivel global, que incluye el RGPD de la UE y la Ley General de Protección de Datos (LGPD) de

Brasil, que proporcionan una lista de fundamentos jurídicos para el tratamiento de datos personales y, por lo tanto, reconocen la importancia y la validez de los fundamentos de interés legítimo para el tratamiento de datos. Sin embargo, los requisitos actuales para el interés legítimo en el artículo 12 (f) se beneficiarían de identificar instancias en las que haya interés legítimo de terceros. Por ejemplo, el RGPD considera la prevención del fraude, la seguridad de la información y la red y las amenazas a la seguridad pública como tipos de tratamiento de datos considerado de interés legítimo.[2] La AAIP debe incluir de manera similar estos fundamentos como bases legítimas para el tratamiento de recopilación de datos personales.

Además, la AAIP debe considerar la recopilación y el tratamiento legítimos de datos personales que tienen fines científicos de investigación o medición o de análisis de una medición, para fomentar las inversiones en investigación y desarrollo de nuevas tecnologías. Por ejemplo, la medición del público independiente se ha acomodado en el mercado digital global. La UE ha incluido disposiciones específicas en diversos instrumentos jurídicos (por ejemplo, la Ley de Mercados Digitales) que reconocen la función que tiene la medición del público independiente para los mercados en línea y de los medios, y protegen el trabajo de los proveedores de mediciones de público independiente. Incentivamos a la AAIP a reconocer del mismo modo las mediciones del público independiente legítimas como una actividad de tratamiento legítima. La implementación de requisitos más contextuales y adaptables y de instancias que consideren los derechos fundamentales y la libertad del titular de datos darán lugar a un entorno más equilibrado de tratamiento de datos.

Derechos de los titulares de datos

El ITI insta enfáticamente a la AAIP a que revise el artículo 32 para extender el período de respuesta de diez (10) a al menos treinta (30) días, en coherencia con otros regímenes de privacidad globales como el RGPD. Este período proporcionaría a las empresas el tiempo suficiente para responder solicitudes de manera detallada y sustancial y permitiría la interoperabilidad de programas de cumplimiento de protección de datos que ya se han adoptado en conformidad con las mejores prácticas. Además, la AAIP debería considerar una extensión de al menos treinta (30) días de ser necesario, siempre que el titular de datos sea notificado para justificar circunstancias extenuantes. La AAIP también debería considerar la implementación de una extensión de dos meses para solicitudes complejas, como el RGPD[3].

Aunque el ITI valora la descripción del artículo 15 sobre la información que se

[2] Consulte los Intereses legítimos del RGPD. https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/

[3] Según el artículo 12 (3) del RGPD, el responsable del tratamiento deberá proveer información al titular de datos sin demoras y en cualquier circunstancia dentro de un mes una vez recibida la solicitud. Es posible que se extienda ese período a dos meses más de ser necesario, con la consideración de la complejidad y la cantidad de solicitudes.

necesita que esté disponible para el titular de datos, consideramos que parte de la información sugerida es poco práctica, como la información de datos de (f) sobre el importador de datos a los titulares. Las interacciones de los titulares de datos son, y deberían ser exclusivamente, con la primera parte que recopiló sus datos (el responsable del tratamiento de datos). Una vez que el responsable del tratamiento de datos exporta los datos para el tratamiento, los titulares de datos no necesitan comunicarse con el importador. La responsabilidad de contratar al importador de datos no debería ser del titular de datos, sino del responsable del tratamiento, que es la parte que en principio recopiló los datos personales. Por lo tanto, el titular de datos no necesita tener acceso a información específica como la identidad o la información de contacto del importador de datos.

Cuando una organización contactar a un encargado para el tratamiento de datos personales en su nombre, el responsable del tratamiento es quien continúa teniendo la posesión y el control de los datos personales. Desde el punto de vista del ITI, no existe una razón evidente para imponer una obligación de transparencia sobre el responsable para que provea información acerca de los encargados del tratamiento de datos. Además, el consentimiento de los titulares de datos no es un requisito para contactar encargados del tratamiento de datos en su nombre. Por lo tanto, la obligación actual de informar detalles acerca de los encargados del tratamiento de datos en el artículo 15 (e) es poco práctico y crearía una responsabilidad desproporcionada para las empresas y no aumentaría el nivel de protección para los titulares de datos. Además, la AAIP debería considerar aclarar el artículo 15 (f) para asegurarse de que la obligación con respecto a los países de destino de informes solo se aplique cuando un responsable transfiera datos personales a un encargado aparte en otra jurisdicción. Debido a la naturaleza de los flujos de datos, existen muchas situaciones en las que los datos viajan a otras ubicaciones alrededor del mundo y aun así se consideran nacionales en su totalidad, con lo cual el encargado del tratamiento de datos está sujeto a la ley argentina.

Asimismo, la AAIP debería revisar el artículo 35 (j) (l). Este artículo permite al encargado actuar como contacto para solicitudes de titulares de datos. El ITI considera que el responsable del tratamiento de datos debería ser el único contacto para solicitudes ya que es quien tiene la responsabilidad de garantizar los derechos del titular de datos. Resaltamos la importancia de que los encargados del tratamiento de datos que asisten al responsable respondan a estas solicitudes y, por lo tanto, incentivamos a la AAIP a limitar la obligación respecto de los encargados del tratamiento de datos para asistir al responsable.

En el artículo 28 del anteproyecto de ley, se debate el derecho de oponerse del titular de datos en una manera amplia. En la mayoría de las normativas de protección de datos, el derecho a oponerse se limita a situaciones en las que a) el tratamiento está basado en el interés legítimo; b) se encuentra un subconjunto de situaciones, en especial aquellas en las que los datos personales se procesan para fines de comercialización directa. Sin embargo, en este caso, la AAIP está

extendiendo el derecho de oposición a todas las situaciones en las que no se otorgó consentimiento (lo que incluiría otros varios fundamentos para el tratamiento además del interés legítimo) y en los casos en los que el tratamiento de datos se realiza con fines publicitarios, comerciales y de comercialización directa. En el primer caso (a), no se requiere derecho de oposición cuando depende de otra base jurídica que no es el interés legítimo. En el segundo caso (b), la aplicación de un derecho de oposición a todos los tipos de publicidad, incluida la comercialización no directa, generaría repercusiones difíciles de soportar, en especial para pequeñas y medianas empresas. El anteproyecto de ley actual presenta varios fundamentos jurídicos para el tratamiento de datos personales y no prescribe cuál es la base jurídica requerida para la publicidad. Nuevamente, el derecho a oposición debería circunscribirse a las situaciones en las que el interés legítimo es la base jurídica para el tratamiento, pero no debería aplicar a las circunstancias en las que el responsable haya elegido otro, como cuando se ofrece la publicidad como un servicio en cumplimiento de un contrato (artículo 12 [b]). Asimismo, los titulares de datos deberían tener derecho a oponerse al tratamiento de sus datos personales “cuando se realiza con fines publicitarios, comerciales y de comercialización directa”.

El otorgamiento de un derecho a oponerse a toda forma de publicidad (incluida la comercial) es demasiado amplia, implica que la publicidad es inherentemente invasiva para la privacidad y que tendrá impactos negativos significativos en las pequeñas empresas y la competencia en Argentina. De hecho, en muchos casos, las empresas pueden ofrecer servicios gratuitos porque están financiados por la publicidad. Esto crea un valor financiero concreto que, con frecuencia, financia herramientas gratuitas disponibles para todos, lo que contribuye al avance económico y social. La publicidad no es inherentemente invasiva para la privacidad, y la industria publicitaria más amplia ha invertido en formas de proporcionar anuncios relevantes para los usuarios y, a su vez, usar una cantidad menor de datos y datos personales agregados o que no se puedan identificar con el usuario de otro modo. El derecho a oposición debería estar bien limitado a abordar inquietudes específicas sobre privacidad en lugar de ensañarse con todas las formas de publicidad que aprovechan los datos personales. Existen maneras protectoras de la privacidad para proporcionar publicidad que deberían excluirse del anteproyecto de ley.

En el artículo 29 del anteproyecto, se consideran situaciones en las que los titulares de datos pueden solicitar la eliminación de los datos personales. Estas disposiciones, si se leen en conjunción con el derecho a oposición (artículo 28), presentan algunas redundancias e incoherencias. En especial, en (f) las disposiciones establecen que los datos pueden ser solicitados para su eliminación si se tratan con fines “publicitarios, comerciales y de comercialización”. Esto contrasta con la norma que se destaca en el artículo 28, en la que se habla de los fines “publicitarios, comerciales y de comercialización directa”.

Si bien consideramos que el artículo 28 debería modificarse, es importante

subrayar que se debería aplicar el mismo criterio a ambos artículos 28 y 29. De hecho, están unidos. Por ejemplo, en (c) se establece que el titular de datos tiene derecho a solicitar la eliminación si ejerce de manera correcta su derecho a oponerse. En este aspecto, el artículo 29 está subordinado al artículo 28, ya que para poder solicitar la eliminación de sus datos, el titular debe tener la posibilidad de oponerse al tratamiento. Si el derecho a oposición está limitado a los casos de "comercialización directa", pero el derecho a eliminación se extiende a todas las formas de comercialización (sin especificar la característica "directa"), en la práctica no coinciden las dos disposiciones. Por otra parte, si se alinean las dos normas (lo cual recomendamos), (f) quedaría en efecto redundante porque (c) ya resalta que el artículo 29 se aplica a los casos alcanzados en el artículo 28.

Deberes del responsable y encargado del tratamiento

Los regímenes de privacidad deberían imponer requisitos diferentes para los responsables y los encargados del tratamiento de datos. Los responsables deberían tener la responsabilidad principal de satisfacer las obligaciones de privacidad y seguridad jurídicas. En contraste, los encargados deberían ser responsables solo de seguir las instrucciones del responsable según lo establecido en sus contratos.

El ITI recomienda que la AAIP revise el lenguaje del anteproyecto de ley para definir las funciones y las responsabilidades de los responsables del tratamiento de datos (quienes determinan los medios y los fines del tratamiento de datos personales) y de los encargados del tratamiento de datos (quienes los tratan en nombre de los responsables), y que aclare que los responsables del tratamiento de datos tienen la responsabilidad principal de la privacidad y seguridad. Por ejemplo, los artículos 8, 11, 19, 35, 36 y 38 imponen obligaciones sobre los encargados del tratamiento de datos que generarían problemas de cumplimiento, ya que los encargados no tienen acceso a la información ni los medios necesario para cumplir con esas obligaciones. Sugerimos que se armonicen las obligaciones que impone el anteproyecto de ley sobre los encargados del tratamiento de datos con otros regímenes de privacidad de datos, como el RGPD[4], que limita esas obligaciones a los responsables del tratamiento.

Notificación de filtración de datos y de incidentes

Argentina debe adoptar un régimen de notificación de incidentes de filtración de datos flexible y preventivo de daños, que incorpore un análisis de riesgo de daños, que diferencie entre la notificación a los titulares de datos (interesados) y a la autoridad pública pertinente, y que evite un enfoque universal que establezca límites de tiempo específicos para la notificación.

Nos gustaría resaltar los enfoques flexibles y razonables adoptados en Singapur y Hong Kong como ejemplos de regímenes de notificación de filtración de datos que son eficaces y practicables. Los requisitos sofisticados en materia de filtración de

[4] Consulte los artículos 5, 24, 25, 28 y 29 del RGPD.

datos reconocen que el mero acto de notificación en sí mismo no produce una mayor seguridad o privacidad para los titulares de datos. Por lo tanto, imponen requisitos de notificación de manera adaptable y dependiente del contexto que permiten evaluar el riesgo de daño, con el objetivo de proteger a las personas en los casos en que se producen infracciones. Recomendamos que la notificación se considere como un posible medio para alcanzar el objetivo final de proteger a los titulares de los datos filtrados y no como el fin en sí mismo.

Una legislación eficaz de notificación de infracciones basada en los daños reconoce el delicado equilibrio entre el exceso y la falta de notificación con respecto al momento en que deben enviarse los avisos a los titulares de datos y permite a las organizaciones comunicarse con sus clientes de manera coherente con las comunicaciones anteriores, en lugar de prescribir un formato específico.

El ITI recomienda que los regímenes de notificación de filtración de datos no impongan límites de tiempo estrictos para la notificación. El artículo 20 del anteproyecto de ley exige que los responsables del tratamiento notifiquen los incidentes en un plazo de 48 horas, un período de tiempo más estricto que el de otros regímenes, como el RGPD que exige 72 horas y la LGPD de Brasil que exige la comunicación en un tiempo razonable [5]. En su lugar, la AAIP debe crear la obligación de notificar sin demora injustificada una vez que la organización haya recabado información, tras tener conocimiento de un incidente. Esto permitiría a las organizaciones realizar las investigaciones necesarias e implementar medidas de mitigación cuando sea necesario, sin tener que restar tiempo valioso a la AAIP para la emisión de informes preliminares que pueden tener que rectificarse después de que la organización en cuestión tenga más información sobre los hechos. Los períodos de notificación breves y prescriptivos no dan a las organizaciones un tiempo razonable para conseguirlo. Además, el artículo 35 (k) del anteproyecto de ley requiere que los encargados del tratamiento notifiquen los incidentes al responsable del tratamiento y al ente regulador “dentro del plazo legal”, pero no define este plazo. La AAIP debe seguir otros regímenes, como el RGPD,[6] y crear una obligación para que los encargados del tratamiento notifiquen al responsable del tratamiento sin demora irrazonable después de tener conocimiento de un incidente. La obligación de notificar debe limitarse al responsable del tratamiento (no al ente regulador) porque el responsable del tratamiento se encuentra en mejor posición para recopilar información sobre un evento de seguridad y el encargado del tratamiento no siempre podrá determinar si los datos se han visto o podrían haberse visto comprometidos.

Las leyes sobre filtración de datos también deben aplicar diferentes criterios para

[5] De acuerdo con el RGPD, los responsables del tratamiento deben notificar determinados tipos de filtraciones de datos personales a la Autoridad de Protección de Datos en un plazo de 72 horas después de tener conocimiento de la filtración. La LGPD de Brasil exige que las notificaciones se realicen en un plazo razonable (artículo 48, párrafo 1).

[6] Según el artículo 33 (2) del RGPD, los procesadores de datos deben notificar determinados tipos de filtraciones de datos personales al responsable del tratamiento sin retrasos injustificados después de tener conocimiento de la filtración de datos personales.

notificar a los entes reguladores y a los titulares de datos. Primero, señalamos que debe preferirse la comunicación con el titular de datos en lugar de la notificación, ya que el objetivo de la información debe ser ayudar a los titulares de datos afectados con recomendaciones sobre cómo proteger los datos personales. Comunicar a los titulares de datos un incidente sin ofrecer a las organizaciones el tiempo necesario para realizar una revisión adecuada de los eventos puede ser contraproducente si se prueba que la presunta filtración es falsa o si esta no crea un riesgo de robo de identidad. Además, la sofisticación de los piratas informáticos de hoy en día y la naturaleza desafiante de una investigación forense posterior a la filtración de datos exigen una legislación que cree requisitos de tiempo realistas, flexibles y factibles. Los datos comprometidos que se encriptan o se hacen inaccesibles de otro modo también deben estar exentos de los requisitos de notificación.

Asimismo, el ITI anima a la AAIP a unificar los conceptos de filtración de datos que se encuentran en los artículos 2, 20 y 34 (h). Esto facilitaría a las empresas una comprensión integral del concepto de filtración de datos. El ITI anima a la AAIP a alinear estos artículos a fin de definir una filtración como una falla de seguridad que conduce a la destrucción accidental o ilícita, la pérdida, la alteración, la divulgación o el acceso no autorizado en torno a los datos personales.

Decisiones automatizadas y elaboración de perfiles

Si bien es necesario contar con disposiciones que protejan a los titulares de datos contra los riesgos derivados de los tipos de elaboración de perfiles que podrían producir daños y que garanticen que el responsable del tratamiento va a asumir sus responsabilidades, el artículo 30 (junto con los artículos 15 y 39) prescribe algunas obligaciones en los casos de la toma de decisiones automatizadas, y aplica explícitamente esos requisitos a las decisiones total y parcialmente automatizadas. Especifica que los titulares de datos tienen derecho a no ser sometidos a decisiones automatizadas cuando estas a) produzcan efectos jurídicos perjudiciales; b) afecten al titular de datos de manera igualmente negativa y c) tengan efectos discriminatorios. También prescribe que un titular de datos tiene derecho a la revisión por parte de una persona física de las decisiones automatizadas cuando afecten sus intereses, incluidas las decisiones que definen los aspectos personales, profesionales, de consumo y de crédito.

El ITI desea señalar algunos problemas con esta disposición. Primero, estos requisitos solo deben aplicarse a decisiones totalmente automatizadas. Debe eliminarse cualquier referencia a las decisiones parcialmente automatizadas en el anteproyecto de ley. Esto se debe a que el uso de la automatización en la economía actual está muy extendido. Es insostenible exigir que los usuarios se excluyan voluntariamente de todos los niveles de automatización. Esto significaría, por ejemplo, que los programas informáticos básicos como las calculadoras o las bases de datos no podrían utilizarse en determinadas situaciones si el usuario renuncia voluntariamente a la toma de decisiones automatizadas. Tampoco trataría las preocupaciones que la AAIP está tratando de abordar con esta disposición, es decir, garantizar que se establezcan protecciones adecuadas en los casos de alto

riesgo, que deben definirse de forma estricta y específica. De hecho, la norma relativa a la toma de decisiones automatizadas debe aplicarse a usos específicos que sean directamente responsables de efectos jurídicos claramente identificados o de importancia similar. Los sistemas parcialmente automatizados, o los sistemas en los que hay una persona involucrada, no cumplen esa norma porque es en última instancia una decisión humana y no automatizada. En la actualidad, las decisiones humanas suelen implicar cierto nivel de automatización (por ejemplo, el uso de una hoja de cálculo o computadora) y dichas decisiones están reguladas por las leyes existentes. Las exigencias elevadas solo deben aplicarse en la toma de decisiones totalmente automatizadas.

Segundo, expresar que el derecho a oposición se aplica a decisiones que tienen "efectos discriminatorios" tiene una connotación peligrosamente general. Muchos sistemas automatizados, por ejemplo, los sistemas de recomendación, discriminan en el sentido de mostrar diferente contenido a distintos públicos debido a su uso y finalidad previstos. Personalizar el contenido que se muestra a los usuarios no solo es legítimo, sino que se ha demostrado su utilidad. Por lo tanto, se debe ajustar el lenguaje para garantizar que las tecnologías legítimas y beneficiarias no se restrinjan indebidamente, y que no se suprima la innovación. Lo que debe evitarse es la discriminación "ilegal" o "ilícita".

Tercero, parece que hay algunas incoherencias en las normas que se utilizan en el anteproyecto de ley para los términos y las disposiciones interconectados. El legislador exige lo siguiente:

a) Derecho a oposición, cuando las decisiones causan efectos jurídicos o de importancia similar, o son discriminatorias.
b) Derecho a la revisión por parte de una persona humana, en el mismo artículo, cuando las [decisiones] "afectan a sus intereses, incluidas las decisiones encaminadas a definir sus aspectos personales, profesionales, de consumo, crédito, de su personalidad u otros".

Estas normas no son homogéneas. Esto puede generar confusión en torno a las obligaciones que se aplican a la situación específica. También requeriría que los responsables del tratamiento realicen una evaluación cada vez que estos derechos se aplican a esa situación particular: si se aplica uno, no se aplica ninguno, se aplican ambos o se aplica solo uno. Esto probablemente disuadirá la innovación, especialmente en las pequeñas y medianas empresas, que necesitan navegar en un entorno altamente incierto, pero también generará confusión e incertidumbre entre los titulares de datos, que están destinados a ser los beneficiarios de la legislación propuesta. También parece una elección poco razonable dentro del mismo artículo: podría decirse que el alcance del artículo es su propio título, es decir, la toma de decisiones automatizadas y la elaboración de perfiles. Los rechazos de esta disposición, incluyendo el derecho a oposición y el derecho a la revisión por parte de una persona humana, deben tener el mismo alcance. No tiene mucho sentido incluir dos disposiciones que no están conectadas entre sí.

La recomendación es que ambas normas se alineen para que sean legales o tengan efectos significativos similares. Este es el enfoque que adoptan la mayoría de las demás leyes de protección de datos, y logra el equilibrio adecuado entre la protección de las personas y la habilitación de los usos beneficiosos de los sistemas automatizados. Además, estas normas producirían una mayor armonización mundial, a diferencia de la alternativa, que daría lugar a problemas de cumplimiento normativo. Este es el mismo enfoque que adopta la AAIP en el artículo 39, que prescribe una evaluación de impacto relativa a la protección de datos cuando se evalúan aspectos personales a través de medios automatizados y cuando esas decisiones producen efectos legales o significativos de otro tipo. Con la advertencia de que la formulación actual abarca las decisiones parcialmente automatizadas, que no deben estar en el ámbito de aplicación, consideramos que la norma es la correcta y señala cómo el ente regulador aborda la evaluación del riesgo para la toma de decisiones automatizadas. Por consiguiente, se debe adoptar un enfoque similar para las demás disposiciones sobre el mismo tema, es decir, en todo el artículo 30.

Por lo tanto, los artículos 26 (i) y 30 necesitan una mayor aclaración acerca de lo que se consideraría información adecuada sobre los criterios utilizados en las decisiones automatizadas. Esta falta de claridad crea incertidumbre jurídica y plantea problemas de cumplimiento normativo.

Sanciones y multas

La responsabilidad es un principio bien establecido de la protección de datos. La responsabilidad desplaza el foco de atención de la gestión de la privacidad hacia las organizaciones, esto les exige aceptar la responsabilidad de recopilar, tratar o usar de algún otro modo los datos personales, independientemente de los requisitos legales. Los modelos vanguardistas de privacidad y protección de datos se centran en cómo los responsables del tratamiento pueden garantizar que sus operaciones de tratamiento no infringen los derechos de las personas ni suponen una carga excesiva para estas. Esta es la base del modelo de responsabilidad de la protección de datos.

Las empresas de todo el mundo están realizando inversiones significativas para poner en funcionamiento el principio de responsabilidad, como la creación de programas integrales de privacidad, la asignación de personal especializado para supervisar los problemas de privacidad y la documentación de las prácticas recomendadas. Recomendamos que los legisladores reconozcan e incentiven estos “buenos actores” y las prácticas de responsabilidad. Por ejemplo, los legisladores podrían ofrecer presunciones de cumplimiento normativo o reducciones de las sanciones a las organizaciones que mantengan dichos programas.

El ITI sugiere que se revise el artículo 58 para garantizar que las sanciones que se apliquen sean proporcionales al grado de daño o riesgo de la acción que justificó la

sanción. Suspender “las actividades relacionadas con el tratamiento de datos personales” puede dar lugar a excesos que perjudiquen gravemente la actividad económica. También creemos que la legislación no debe dar lugar la interpretaciones equívocas por parte de la autoridad de aplicación. El artículo 58 (d) incluye una sanción que consiste en el cierre temporal de las operaciones. No está claro si hace referencia a las operaciones de tratamiento de datos o a las operaciones comerciales. Recomendamos a la AAIP que aclare el concepto de “operación” para que se restrinja a “una limitación temporal o definitiva, incluida la prohibición de tratamiento de datos”.

Además, la AAIP debe revisar el artículo 60 para garantizar que las multas también sean proporcionadas. Usar los ingresos mundiales de una empresa como base para el cálculo de multas es excesivo y podría disuadir a las empresas de ofrecer productos y servicios innovadores a los usuarios de Argentina. En cambio, la AAIP debería considerar la posibilidad de utilizar los ingresos locales de la empresa como otros mercados regionales, como Brasil[7].

Otras recomendaciones discretas

- **Representante local en Argentina (artículo 44).** En lo que respecta a la exigencia de una representación en el país para el responsable o encargado del tratamiento, la AAIP debe considerar y flexibilizar la cobertura de varias situaciones, especialmente porque la presencia local por sí misma no es necesaria para garantizar el cumplimiento normativo y una respuesta oportuna. Exigir una representación en el país exclusivamente para estos fines puede resultar oneroso cuando los servicios se prestan desde el extranjero y actuar como una barrera de acceso al mercado. Por lo tanto, el ITI recomienda un enfoque moderno como los que se aplican en Japón, Nueva Zelanda y Brasil, donde no hay requisitos específicos para un representante de responsable o encargado del tratamiento. Asimismo, en caso de que esta disposición permanezca en el texto, sugerimos que se supriman las responsabilidades personales. Esto atentaría claramente contra las posibles decisiones de inversión en el país e impediría el desarrollo de una cultura de protección de datos basada en la responsabilidad. Es difícil imaginar la aparición de un grupo amplio y competente de profesionales locales que asuma dicha responsabilidad. Además, para garantizar la seguridad jurídica y evitar malentendidos, también sugerimos mencionar explícitamente que se excluye la responsabilidad penal.

- **Registro Nacional para la Protección de Datos (artículo 45).** Los registros centralizados, como el que propone el artículo 45, ya no son las mejores

[7] El artículo 52 de la Ley General de Protección de Datos Personales de Brasil establece una multa de hasta el dos por ciento de los ingresos de una persona jurídica privada en Brasil, sin excederse de BRL 50 000 000,00 por infracción.

prácticas en las leyes de protección de datos modernas. La AAIP evidentemente reconoció esto, ya que no incluyó un registro nacional de bases de datos en el proyecto de ley propuesto y derogó la Ley N° 25.326, que creó el registro nacional de bases de datos existente. Hay varias herramientas existentes que le permiten a la AAIP tener acceso a la información de las partes interesadas en el tratamiento de datos. Sin embargo, la creación de un registro nacional para la protección de datos para responsables y encargados del tratamiento aumentaría los costos para la AAIP y las empresas de la cadena de suministro de tratamiento de datos sin aportar ningún beneficio adicional desde el punto de vista de la protección de datos. Por consiguiente, el ITI recomienda que la AAIP elimine de la legislación las obligaciones de registro de los responsables y encargados del tratamiento mediante la supresión por completo del artículo 45. Esto reflejaría la decisión adoptada por la mayoría de las jurisdicciones de todo el mundo que ahora han abandonado esta práctica y consideran que aporta poco valor real, como el RGPD.

- **Medidas para la protección de datos personales (artículo 19).** La industria apoya firmemente la implementación de la evaluación y mitigación de riesgos. Sin embargo, el lenguaje presente en el proyecto de ley podría ser más preciso para determinar que los responsables y encargados del tratamiento solo están obligados a implementar medidas que se consideren apropiadas para prevenir los riesgos que identifiquen como potenciales para sus actividades de tratamiento de datos.

- **Deberes del responsable y encargado del tratamiento (artículos 34 y 35).** El ITI recomienda a la AAIP que revise el lenguaje del artículo 34 (b) a fin de evitar la creación de problemas de cumplimiento normativo y regímenes conflictivos. Tal como está redactado actualmente, el artículo 34 (b) no tiene en cuenta determinadas limitaciones en torno a la eliminación de datos personales específicos, como datos fiscales y sanitarios. De manera similar, el artículo 35 (d) impone una limitación de dos (2) años para el almacenamiento de datos, lo que puede entrar en conflicto con otras obligaciones legales y normativas que debe cumplir el encargado del tratamiento. Por lo tanto, el ITI insta a la AAIP a alinear este requisito con otras leyes para que se permita a los encargados del tratamiento mantener los datos durante el tiempo que exigen otras leyes aplicables. Este límite estricto de 2 años haría imposible que los encargados cumplan con otras obligaciones legales y normativas. Por lo tanto, el ITI sugiere la siguiente línea de edición:

    - “(d) Una vez cumplida la prestación contractual, los datos personales tratados deben ser devueltos al Responsable o destruidos, salvo que medie autorización expresa del Responsable cuando razonablemente se pueda presumir la posibilidad ulteriores encargos, en cuyo solo podrán conservarse **según lo requiera la ley aplicable**”.

Asimismo, el artículo 35 (e) establece que el responsable del tratamiento tendrá permitido realizar inspecciones y auditorías. El ITI recomienda que se aclare que esta obligación puede cumplirse mediante informes de terceros independientes[8]. El artículo 35 (e) también establece que la autoridad de aplicación debe estar autorizada a realizar inspecciones y auditorías a fin de verificar el cumplimiento con la legislación. Para crear mayor seguridad jurídica, el proyecto de ley debe ser más específico a la hora de identificar cuándo y en qué circunstancias la AAIP tendría autoridad para realizar auditorías y especificar el proceso jurídico que deberá seguirse. Además, las auditorías deben requerir una orden judicial que garantice el proceso debido y contemple las objeciones a las inspecciones y auditorías de la organización.

El artículo 35 (f) menciona que los encargados del tratamiento no pueden usar subcontratistas sin "consentimiento expreso". Este requisito va más allá que otros regímenes de protección de datos, como el RGPD y podría provocar problemas de cumplimiento normativo[9]. El ITI recomienda que el anteproyecto de ley permita una autorización general. Los incisos (g) y (h) del artículo 35 imponen al encargado del tratamiento obligaciones de seguridad que deben recaer sobre el responsable del tratamiento. El ITI recomienda que el anteproyecto de ley limite las obligaciones de seguridad de los encargados del tratamiento a la implementación de medidas técnicas y organizativas apropiadas[10]. Los incisos (j) y l) del artículo 35 obligan a los encargados del tratamiento a responder a las solicitudes de los titulares de datos. Sin embargo, los encargados del tratamiento no tienen relación con los titulares de datos y es posible que no tengan acceso a la información de tales titulares ni puedan confirmar la identidad de los interesados. En cambio, el ITI recomienda que el anteproyecto de ley siga otros regímenes de datos, como el RGPD, y solo exija que los encargados del tratamiento ayuden a los responsables del tratamiento a responder a las solicitudes de

[8] Consulte el lenguaje en el art. 28.3 (h) del RGPD: [Dicho contrato u otro acto jurídico estipulará, en particular, que el encargado del tratamiento:] "ponga a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, permita las auditorías y contribuya a tales auditorías, incluidas las inspecciones, realizadas por el responsable del tratamiento u otro auditor que ordene el responsable del tratamiento".

[9] Consulte el lenguaje en el art. 28.2 del RGPD: "El encargado del tratamiento no podrá contratar a otro encargado sin la previa autorización escrita específica o general del responsable del tratamiento. En el caso de la autorización escrita general, el encargado del tratamiento informará al responsable del tratamiento cualquier cambio previsto relativo a la incorporación o el reemplazo de otros encargados del tratamiento, lo que brindará al responsable del tratamiento la oportunidad de oponerse a tales cambios".

[10] Consulte el art. 32 del RGPD.

los titulare de datos en la medida de lo posible[11].

- **Datos de los menores de edad (artículo 18).** El anteproyecto de ley actual estipula que los menores de 13 años pueden dar su consentimiento para el tratamiento de sus datos solo cuando los datos se utilicen para la obtención de información relacionada con la prestación de servicios específicamente diseñados y adaptados a los niños. También establece que los responsables del tratamiento no pueden tratar los datos de los niños o adolescentes para juegos, aplicaciones u otras actividades más allá de lo estrictamente necesario para el desarrollo de esa actividad.

  El ITI está de acuerdo en que los menores de edad son titulares de datos por derecho propio y que el tratamiento de los datos de los menores debe basarse en el principio del "interés superior del niño". También estamos de acuerdo en que la presente ley debe estar respaldada por un principio de neutralidad tecnológica (según el artículo 5) y por un enfoque basado en los riesgos. Sin embargo, el texto actual parece contradecir ambos. Por lo tanto, recomendamos que la AAIP centre estas disposiciones en torno al criterio del "interés superior del niño". El principio del interés superior del niño es una perspectiva importante a través de la cual se pueden ver y equilibrar los diferentes derechos conferidos a los niños en virtud de la Convención de las Naciones Unidas sobre los Derechos del Niño (UNCRC, por sus siglas en inglés), que incluyen, entre otros, el derecho a la privacidad. Centrar el criterio del "interés superior del niño" en todas las consideraciones garantiza un equilibrio apropiado entre la protección de la privacidad, la seguridad y el bienestar de los jóvenes, y su empoderamiento con herramientas para expresarse, acceder a información y crear una comunidad en línea. También sugerimos que se haga hincapié en un enfoque basado en el riesgo en todos los aspectos relacionados con el tratamiento de los datos personales de los jóvenes. Dicho enfoque es fundamental para evitar los posibles inconvenientes de ciertos tipos de tratamiento de datos para los jóvenes, al tiempo que les permite disfrutar de los beneficios de los servicios modernos basados en datos. Esto garantizaría que el criterio del "interés superior del niño" se aplique de manera adecuada en todos los aspectos.

  El principio del interés superior del niño exige una evaluación integral de los hechos y las circunstancias. Es posible que determinados tratamientos (por ejemplo, para garantizar la seguridad de una plataforma) afecten, de manera proporcionada, los derechos de privacidad de los niños, pero pueden ser necesarios para permitir o facilitar actividades que, en conjunto, redundan en

[11] Consulte el art. 28.3 (e) del RGPD: [Dicho contrato u otro acto jurídico estipulará, en particular, que el encargado del tratamiento:] "teniendo en cuenta la naturaleza del tratamiento, asista al responsable del tratamiento mediante medidas técnicas y organizativas apropiadas, en la medida en que ello sea posible, para el cumplimiento de la obligación del responsable del tratamiento de responder a las solicitudes relativas al ejercicio de los derechos del titular de datos que se mencionan en el capítulo III;

el interés del niño (como permitir a los niños comunicarse con sus pares o protegerlos de posibles riesgos).

- **Período de gracia (artículo 72).** Desde el punto de vista de la aplicación, recomendamos enfáticamente que la AAIP amplíe el período de cumplimiento de un (1) año a dos (2) años, como mínimo, a fin de permitir que las empresas tengan tiempo suficiente para cumplir con los requisitos, de forma similar al período de implementación estipulado en el RGPD.

Salta, 11 de octubre de 2022

Sra. Directora

Lic. Beatriz de Anchorena

Agencia de Acceso a la Información Pública

S / D

Tengo el agrado de dirigirme a Usted, en mi carácter de Director del Instituto de Derecho de las Telecomunicaciones, Informática y Nuevas TICs del Colegio de Abogados y Procuradores de la Provincia de Salta, a fin de acercarle la opinión del Instituto que represento en la relación a la consulta formulada por Resolución 119 de 2022 de la Agencia a vuestro cargo, para el anteproyecto de nueva ley de protección de datos personales presentado.

Este Colegio viene trabajando ya desde hace casi diez años sobre la temática, desde su Instituto específico, y es intención generar propuestas serias y valederas que ayuden a lograr el mejor proyecto posible para el tratamiento de nuestros datos personales. Un proyecto moderno, dinámico, transparente, abarcativo, en sintonía con lo que el mundo ha ido normando en la materia; así lo amerita.

Desde este punto de vista, consideramos que, esta fuera de discusión la oportunidad o no de la actualización y/o modificación de nuestra ley vigente, la 25.326. En los tiempos que corren y habiendo transcurrido mas de 20 años de sancionada la misma, una reforma

tendiente a proteger los datos personales de los argentinos, en la era de la tecnología, urge.

Las condiciones no son las mismas hoy que en el 2000, las redes sociales, y no solo ellas, estallaron y los datos circulan por todos lados (Facebook, posiblemente la red social más emblemática, aunque parezca de toda la vida, inició su actividad recién en 2004). La actividad económica se mueve y se cotiza en datos, los cuales conforman el principal insumo de la llamada economía del conocimiento. Grandes cantidades de información digital son controladas por gobiernos, por empresas o distintas organizaciones. Datos de valor económico, social, que en la actualidad resulta imperioso resguardar. Entiéndase bien, resguardar no inmovilizar; los necesitamos móviles, vivos, activos, pero también seguros.

Muchos países del mundo, desde distintas ópticas o bajo miradas diversas, abordaron el problema y avanzaron en regímenes de protección integral de sus datos personales.

Nuestro país debe avanzar en dos sentidos, que no se contraponen para nada. Debe resguardar, garantizar, el ejercicio del derecho fundamental de las personas humanas a la protección de sus datos personales y su privacidad, pero también debe proteger la innovación, la creatividad, los desarrollos que las tecnologías nos traen.

En nuestro país hubo intentos de legislar, de actualizar la temática, pero cayeron en saco roto por mezquindades políticas bastante absurdas. Hoy, la Agencia de Acceso a la Información Pública (AAIP), con muy buen criterio, vuelve a poner la materia en el centro de la escena, al presentar un Anteproyecto de ley de protección de datos personales y privacidad que, en general, sigue las tendencias actuales en el mundo al respecto.

Mas allá de los lineamientos que sigue el Anteproyecto que, en general, consideramos correctos, creemos que esta protección debe tener como eje a la persona; el hombre como centro, no la base de datos. Es importante este cambio de mirada, este objetivo de priorizar a los ciudadanos garantizándoles la protección de sus datos personales y su privacidad.

Anonimización de los datos, transparencia, métodos de responsabilidad proactiva, de rendición de cuentas, consentimiento informado, la necesaria intervención humana en el tratamiento automatizado de datos, la autodeterminación informativa, la protección colectiva (¿porque no?), deben ser sin duda abordados. Algunos temas están, a otros les falta precisión, unos pocos no están y creemos debemos incluirlos.

Es significativo el alcance territorial del Anteproyecto que incluye a los responsables de datos que no están en nuestro país, obviamente bajo ciertas condiciones como la de realizar el tratamiento de los datos en nuestro territorio, o en aquellos casos en que el derecho internacional o contractual hace aplicable nuestra legislación. Tener esto en cuenta en la era de la tecnología es una premisa y en variados ámbitos internacionales se está abordando la cuestión. Si bien enfocado en la temática del cibercrimen, Budapest, su convenio y su protocolo adicional así nos lo muestran.

Y en este mirar a la persona, es trascendente también el tratamiento de los datos de menores. Básicamente, sin su consentimiento expreso o el de sus representantes legales no se podrán tratar los datos sensibles de una persona de 13 años o de un adolescente.

En ese deber contemplar y lograr conciliar el derecho a la protección de datos personales y la libertad de expresión y el derecho a la información que creemos necesario, si bien no se prevé el derecho al olvido (en el cual creemos se podría avanzar), se amplía el catálogo de

protección en cuanto a la rectificación, la actualización, la supresión de datos, la oposición y otras figuras consecuentes con ello.

La incorporación del delegado de protección de datos personales, del representante (ante la ausencia en nuestro país del responsable o encargado del tratamiento de los mismos), la proactividad que se exige al responsable del tratamiento de los datos, la obligatoriedad de dejar documentadas las medidas adoptadas en el tratamiento de los mismos, las auditorias tanto internas como externas exigidas, la creación del Registro Nacional para los responsables y encargados del tratamiento que deban designar un delegado de protección de datos o que tengan que tener un representante en nuestro país, constituyen todas medidas auspiciosas.

No menor resulta el hecho de aumentar el valor de las multas y fijar un sistema de actualización basado en una unidad móvil actualizable anualmente; multas estas, fijadas por la AAIP que continua como autoridad de control en la materia. Es de esperar que, a partir de la eventual vigencia de la nueva ley, la autoridad de aplicación ejerza de forma más decidida su rol de supervisión y sanción que es la forma – junto con la educación de la ciudadanía en el valor y la protección de sus datos personales, otra asignatura pendiente – en que otros países han desarrollado una cultura de datos.

En fin, una nueva ley, moderna, equilibrada, robusta, acompañada de políticas de difusión y divulgación, capacitación y fortalecimiento de la actuación de una Agencia independiente, actuando desde el rol técnico que le compete, es fundamental frente a la tecnología; la tecnología que nos invade y a veces nos abruma, pero que, nadie lo duda, resulta totalmente necesaria.

Efectuados estos iniciales comentarios, y con el anteproyecto en mano, vamos a tratar específicos agregados,

modificaciones o supresiones a algunos de los artículos en análisis que este Instituto se permite sugerir.

En su artículo primero el anteproyecto de ley define su objeto: garantizar el ejercicio del derecho fundamental de las personas humanas a la protección de sus datos personales y su privacidad. Abarcativo, pero se podría hacer mayor hincapié quizá en la autodeterminación informativa y agregársela directamente también como objeto de la ley. Ese derecho de la persona a decidir o autorizar de forma libre, previa, expresa e informada la recolección, uso o tratamiento de sus datos personales o de conocer, actualizar, rectificar, suprimir o controla lo que se hace con su información, debiera ser el real y verdadero objeto de la nueva ley de protección de datos personales de Argentina. Desde otro punto de vista, se debiera también remarcar como objeto de la ley la protección plena e integral de los datos, algo simple y sencillo; y, que no se sobreentiende. Mas vale que sobre pero que no falte, suele decirse. Debiera preverlo el objeto de la ley, expresamente.

En cuanto a las definiciones del artículo 2do., no se entiende claramente que significa anonimización, hay un alto grado de indefinición, de imprecisión, de vaguedad o ambigüedad. Quizá se lo podría haber definido más técnicamente para evitar discusiones futuras

El consentimiento del titular de datos esta bien definido en este artículo 2do. Pero se va licuando en artículos posteriores. Esta claro que la tendencia apunta a incluir el consentimiento expreso; pero, en el artículo 12, lo tomamos como una más de seis condiciones y en el 13 nos olvidamos directamente de la palabra “expreso”. Tiene que quedar bien claro que el consentimiento del titular de los datos para que se traten sus datos personales tiene que ser expreso.

En cuanto a personas incluidas en el artículo 2do., cuando se define datos personales; se excluye, en el anteproyecto, a las personas de existencia ideal como titulares de datos protegidos. Esta protección de los datos de las personas jurídicas está prevista en otras legislaciones (Austria, Italia, Suiza) y ha sido reconocida y aplicada con acierto por la jurisprudencia nacional (puede verse sólo de este año 2022, entre otras, CNCom., Sala B, 29/6/2022, Distrisam SA c/ Banco Santander Río SA s/ordinario – Expte. COM 26962/2016; íd., 14/03/2022; Bedmar SA c/ Banco Credicoop Cooperativo Limitado s/ sumarísimo" Expte. 8898/2018; íd. Sala C, 10/2/2022 "Vivian Hnos. SA c/ Cobrex SA y otros s/ sumarísimo" – Expte. nº 27373/2019). Como se observa de estos y otros pronunciamientos, este reconocimiento sigue siendo muy valioso, en particular para la protección de los datos crediticios y financieros de las personas jurídicas además de ya constituir parte del acervo del derecho argentino en la materia. Con lo cual, se propone el mantenimiento de las personas jurídicas dentro de la definición de datos personales y de la protección provisto por esta área jurídica.

Se incluye a las personas fallecidas cuyos derechos son reconocidos en el art. 32 del anteproyecto.

Entre los datos personales sensibles, si bien se amplia el listado (genéticos, biométricos, etc), no se incluyen datos tales como los provenientes de geolocalización, por ejemplo, algo tan común hoy en día.

De todas formas, hubiera sido bueno que mas que listar algunos casos puntuales, se parametrizara cuales son los criterios para identificar a un dato como sensible ahora y a futuro. La Dra. Fallero habla de basar, por ejemplo, la sensibilidad en los estudios de criticidad de datos y no solo en la sensibilidad entendida por los conceptos que vienen mas de las ciencias

sociales, camino que, compartimos, se podría haber seguido en esto de parametrizar los criterios para definir o identificar un dato como sensible.

La perspectiva de género, por ejemplo, es mencionada dentro de los datos sensibles, pero luego el texto no hace alusión a la misma. ¿Los hipervulnerables? Quizá pudiese haberse hecho alusión a ello o por lo menos si se hubiese parametrizado la cuestión los podríamos encontrar incluidos en la norma.

En cuanto a los datos relativos a antecedentes penales y contravencionales de particulares, debería haberse limitado como utilizarlos. Anteriormente se los incluía como categoría de datos sensibles. Hoy no tenemos regulación específica sobre esto. Hay muchas categorías de datos como este que deberían haber tenido tratamiento específico.

En cuanto a los datos de los trabajadores, la ley de teletrabajo ni la de contratos de trabajo cubren estas situaciones. Hoy en día hay vigilancia electrónica sobre los trabajadores. ¿A dónde van a quedar amparadas estas situaciones, en el interés legítimos de los empleadores? No podemos no preveer esto, sería realmente ir contra todos los principios protectorios no tratarlo.

Cuando se define a las entidades crediticias, quizá el banco central de la republica quede como probablemente insuficiente frente al nuevo entorno cripto y Fin Tech no alcanzado por la obligación de compartir información con el BCRA. Pueden existir ficheros privados que provean servicios de información crediticia fuera del radar del BCRA.

En cuanto a grupo económico la definición es imprecisa. No se entiende la referencia a denominación, domicilio, etc. Debería alinearse con el art. 33 LGS.

En la definición de tratamiento de datos, si bien la enumeración es enunciativa, significativamente falta la indexación como tratamiento específico, una de las fuentes de mayor conflictividad por la actividad de los motores de búsqueda de internet. Esta mencionada sin embargo en el art. 4.b.1 del anteproyecto, pero la sugerencia es su inclusión expresa dentro de la definición de tratamiento de datos.

En el último párrafo del artículo 3 (ámbito de aplicación) se habla de que tampoco serán aplicables las disposiciones de la ley a la información anónima ni a los datos anonimizados, de forma tal que el titular de los datos no sea identificable. Acá debiéramos aclarar que, esto, siempre y cuando la anonimización no sea reversible.

En el capitulo 2, de los principios que rigen el tratamiento de los datos personales (por más que el titulo sea otro), al hablar del plazo de conservación, lamentablemente no se establece un plazo. Se hace una referencia al tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento, pero no se fija parámetros mas precisos a seguir. Otra oportunidad perdida para evitar futuros conflictos interpretativos.

Ya hicimos referencia al artículo 12 y su interpretación del consentimiento expreso. No se lo pone como regla. El consentimiento estaba bien definido antes, decíamos, pero, con el avance del proyecto, voy deformando esa definición. Me olvido de la palabra “expreso”. Acá puntualmente el artículo 12 trata al consentimiento como una de seis condiciones o situaciones, muy por el contrario de lo que se esperaba. Se señalaba, en las discusiones previas, la posibilidad de reducir las excepciones al consentimiento. No solo no paso esto, sino que se ampliaron cuestiones que pueden ser muy peligrosas o generar prácticas abusivas. Varias ONGs y organizaciones académicas habían señalado la necesidad de quitar la condición b). Se incluye asimismo el interés legítimo del responsable del tratamiento, inciso f), como una nueva

excepción. Muy impreciso, por lo que será importantísima la demostrabilidad. Igualmente, se podría haber previsto con más precisión la cuestión.

El 13 se olvida de la palabra expreso, ya lo habíamos dicho. Omisión grave. El consentimiento tácito invierte la carga de la prueba, toma al silencio como aceptación lo cual toma como cierto algo que ya superamos, algo desactualizado, que no se encuentra en sintonía con nuestro sistema constitucional actual y con relaciones asimétricas de poder existentes, que serían desvirtuadas de admitirlo (consumidores, relación médico-paciente, etc.)

Biometría, vigilancia facial, etc. fueron declarados inconstitucional por la corte en la ciudad de Buenos Aires pues pervierten nuestro estado de inocencia; todos estamos en estado de sospecha, se invierte la carga de la prueba. Son cuestiones que no deben ser pasadas por alto; no podemos establecer, entre la temática de consentimiento informado, solo como una condición más al consentimiento expreso.

La norma que se proyecta no se ha desprendido entonces de la laxitud de las excepciones al consentimiento. Todas las excepciones debieran ser restrictivas, limitativas. La amplitud de la anterior norma dio lugar a grandes abusos en materia de protección de datos personales. Los abusos en la pandemia, por ejemplo, con aplicaciones que nos pedían datos sensibles sin ningún problema. Estamos en la oportunidad de corregir el rumbo. Este proceso nos los pide.

En el artículo 15 continuamos con la omisión de informar al titular que se hace con los datos, con sus datos. No ayuda obviamente esto a la transparencia del sistema.

En el 18 se encuentra un buen agregado, una asignatura pendiente, que ya sosteníamos constituye la regulación del tratamiento de los datos de niñas, niños y adolescentes.

Si bien el 19 habla del principio de seguridad de los datos personales, esta es otra asignatura pendiente. No hay, hoy, medidas de seguridad obligatorias, solo meras recomendaciones, potestativas, discrecionales de quien debe adoptarlas. Entre los factores a considerar por el responsable o encargado del tratamiento para adoptar medidas de seguridad, está el inciso e) (los incidentes de seguridad previos ocurridos en los sistemas de tratamiento). Si yo no tuve ninguno, no significa que no deba adoptar medidas de seguridad, no haber tenido incidente alguno no prueba que yo cumplí con la seguridad de los datos. Las medidas de seguridad para el tratamiento de los datos personales deben ser vistas como una obligación y un derecho de los titulares de los datos.

El articulo 20 habla de la notificación de los incidentes de seguridad. Tenemos continuamente ciber incidentes y lamentablemente la transparencia informativa brilla por su ausencia. No solo exigirla al sector privado, sino que también debemos hacerla un deber del sector público. La gente no conoce que paso con los últimos ciber incidentes que ocurrieron, no conoce como se resolvieron o las medidas adoptadas, si se solucionaron o no. Deberíamos establecer el nivel de notificación y de comunicación en materia de incidentes de seguridad.

Los artículos 23 y 24 (transferencias internacionales), con buen criterio, siguen al RGPD.

El capítulo siguiente trata de los derechos de los titulares de datos. Si bien se amplió el derecho de los titulares de datos, hay grandísimos ausentes y notables silencios. El más notorio es el tema del derecho al olvido. En materia de supresión de datos no se menciona. Otro ausente más complejo, en lo que respecta al derecho de supresión establece algunas limitantes en las cuales no podrá ejercerse y no se hace mención expresa del derecho a la libertad de expresión y del acceso al información y prohibición de

censura previa. Dos derechos de tal envergadura necesitaban una mención expresa. El derecho al olvido podría desprenderse del art. 9 que prohíbe el tratamiento de datos desactualizados (recordemos que indexar es un tratamiento específico e independiente) pero hubiera sido conveniente una mención expresa. Por otro lado, el reciente fallo "Denegri" de la CSJN no impide el derecho al olvido cuando se trata de una persona privada perjudicada por la indexación de un dato desactualizado conforme al supuesto de hecho por ejemplo del fallo Google Spain/ Costeja González del TJUE. De hecho, la Corte menciona que falla como falla porque no hay normativa que regule este derecho. Era la oportunidad para que la hubiera.

En el artículo 30, referente a decisiones automatizadas y elaboración de perfiles, se establece el derecho del titular de los datos a no ser objeto de una decisión basada pura y exclusivamente en el tratamiento automatizado de datos, pero supeditada a que no produzca efectos jurídicos perniciosos. Pero, ¿quién determina esto? No lo dice. Otro capítulo más de impresiones que pueden preverse y evitar futuras arbitrariedades, inseguridad jurídica. Debemos tener pautas más precisas al respecto. Cuando da la facultad al interesado de solicitar la revisión por una persona humana, no dice quien es esa persona humana, como la vamos a elegir, como vamos a evitar la parcialidad. No dice nada de la ampliación injustificada de los plazos en relación al régimen anterior.

En el artículo 34 referente a los deberes del responsable de tratamiento, también se podría haber incluido el derecho al olvido ya referenciado. Pero, nada.

El artículo 36 nuevamente nos llama a la reflexión sobre ¿cómo se recaba el consentimiento? ¿Es válida su aceptación solamente por navegar por el sitio web que tenga publicada la política de privacidad como ocurre en la actualidad, es decir, mediante un browse wrap? ¿O

es necesario un consentimiento efectivo (click wrap o similar) ?; el consentimiento expreso, tantas veces declamado, pero imprecisamente proclamado.

La evaluación de impacto del 39 sigue al RGPD, no constituye novedad, pero está muy bien que se prevea.

En cuanto al delegado de protección de datos, al igual que tampoco le exigíamos al delegado nacional, prácticamente no se le exige idoneidad específica, profesional, alguna.

El artículo 45 establece el registro nacional para la protección de datos para los responsables y encargados del tratamiento que conforme al 42, deban tener un delegado de protección de datos y para quienes conforme al 44 deban contar con un representante en Argentina, pero no establece ya la obligatoriedad de registro de las bases de datos.

La existencia de un capitulo especifico para los datos de información crediticia y el deber de comunicación del 49, quizá era algo novedosos para la época de la anterior ley, no para hoy. Junto a esto debió regularse muchísimas cosas más, los algoritmos están presentes en muchísimos otros sectores que exceden a este.

Una ley de protección de datos personales, fuerte, robusta, debiera contar con una autoridad de aplicación en sintonía. En acceso a la información pública existen principios contrapuestos a la privacidad de los datos personales. No hay una autoridad con idoneidad específica en la materia, sino que comparte otros quehaceres y en el conflicto podríamos prever para qué lado se inclinará. Mas allá de eso, una ley de tal envergadura merecería una autoridad específica.

Saldada la deuda de establecer sanciones, nos damos con la novedad que las multas no se aplican a los

incumplimientos estatales. Debieran aplicarse pues es el estimulo a cumplir. Nulla poena sine lege, frase latina más vigente que nunca.

En cuanto a la declaración de orden público de la norma y su aplicación en todo el territorio es un cambio sustancial. Con el régimen anterior cada provincia era invitada a adherir y regulaba su habeas data, por ejemplo.

Para ir cerrando y volviendo a un ejemplo cercano en el tiempo, el censo pedía nombre DNI y edad. Por otro lado, para mantener el subsidio de los servicios públicos debíamos renunciar a otros derechos. No hubo pronunciamientos públicos al respecto.

Hay muchísimas deudas en cuanto a regímenes específicos, como ya veíamos. Tenemos que ver la normativa complementaria, internet de las cosas, por citar solo un ejemplo. Esta bueno que basemos la nueva protección en un derecho mas moderno. Debemos reconocerlo de forma expresa. Debemos abrazar nuevos derechos y situaciones protectorias que, como sostuvimos no están reconocidas en el anteproyecto.

Por qué no hablar acá también de figuras que legislación moderna ha ido incorporando, el daño punitivo, por ejemplo. ¿Por qué no incorporar también las astreintes?

En síntesis y efectuadas las observaciones concretas, solo decir que quizá podamos mejorar en el proyecto definitivo la visión técnica real de la cosa, lograr ampliaciones y/o mayor precisión en los aspectos soslayados o poco claros ya detallados. Debemos evitar dejar abierto el conflicto. En cuanto mayor precisión demos a las definiciones, menor posibilidad de conflictos jurídicos futuros tendremos.

Luego de este apurado compendio, quedamos a disposición para futuras ampliaciones y/o aclaraciones que redunden en una mejor, más moderna y adecuada ley de protección de datos personales para nuestro país.

Saludamos a la Sra. Directora muy atentamente y la felicitamos nuevamente por el proceso participativo emprendido.

Ciudad Autónoma de Buenos Aires, 11 de octubre de 2022

NOTA Nº S22002129

Sra. Directora de la
Agencia de Acceso a la Información Pública
Mg. Beatriz Anchorena

Tenemos el agrado de dirigirnos a Ud. en nuestro carácter de representantes del Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires con motivo de la consulta pública referida al anteproyecto de Ley de Protección de Datos Personales establecido en la Resolución AAIP 119/2022 y el Reglamento General para la Elaboración Participativa de Normas, Anexo V del Decreto 1172/03.

Las Comisiones de Estudio de nuestro Consejo Profesional constituyen un espacio fundamental para el análisis de normas que involucran el ejercicio profesional y el desarrollo de conocimientos técnicos. En este sentido, hemos puesto a consideración el contenido del anteproyecto mencionado anteriormente y de su tratamiento surge la siguiente recomendación:

- Incluir a los Contadores Públicos como profesionales intervinientes en los mecanismos de certificación en materia de protección de datos establecidos en los artículos 24, 46 y 51 del anteproyecto sobre la base de aplicación del nuevo texto de la Resolución Técnica FACPCE Nº 37 "Normas de Auditoría, Revisión, Otros Encargos de Aseguramiento, Certificaciones, Servicios Relacionados e Informe de Cumplimiento", el cual establece (Capitulo V. Normas sobre Otros Encargos de Aseguramiento, Sección A. Otros Encargos de Aseguramiento en General, Apartado i Normas para su desarrollo) que: *"En los encargos de aseguramiento del presente capítulo, la materia objeto de análisis o evaluación puede adoptar muchas formas, entre ellas:… 14.4. Sistemas de control interno referentes a tecnología de información de una entidad… 14.5.Sistemas de control interno de tecnología de la información referentes a seguridad, disponibilidad, integridad de procesos, confidencialidad y privacidad de la información, implementados u operando en organizaciones prestadoras de servicios informáticos en forma remota a entidades usuarias".*

Es importante destacar que desde el año 2006 nuestra Institución trabajó en conjunto con la Dirección Nacional de Protección de Datos Personales y en el año 2011 se logró implementar un convenio de colaboración que permitía que los profesionales matriculados y las sociedades de profesionales registradas en nuestra institución pudieran cumplir con su obligación de declarar sus bases de datos a través de un mecanismo simplificado de inscripción habilitado a tal efecto.

Asimismo en el marco de colaboración permanente, nos ponemos a disposición y le hacemos saber nuestro interés en llevar adelante los trabajos que permitan dialogar respecto de las principales cuestiones inherentes al rol de los profesionales en Ciencias Económicas y su contribución a la sociedad.

Quedando a su disposición y sin otro particular, la saludamos a Ud. muy atentamente.

Silvia Abeledo
Secretaria
CP 143/42

Gabriela Russo
Presidenta
CP 317/248
LA 47/56

GCTyAP/DN