PDP

Dirección Nacional de
Protección de Datos Personales

Ley de Protección de los Datos Personales en Argentina

Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma

Agosto-Diciembre 2016

Subsecretaría de **Asuntos Registrales**

Justicia 2020

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

INDICE

PRESENTACIÓN

La Dirección Nacional de Protección de Datos Personales (en adelante "DNPDP") es la autoridad de aplicación de la Ley N° 25.326 (Ley de Protección de los Datos Personales). El ámbito de la competencia de la DNPDP surge de la ley citada y de la normativa que la reglamenta, fundamentalmente el Decreto Nº 1558/01.

La protección de los datos personales se encuentra garantizada en la República Argentina a través de la acción de hábeas data, incorporada en oportunidad de la Reforma Constitucional del año 1994 en el artículo 43, tercer párrafo, de la Constitución Nacional. Posteriormente se sancionó la mencionada Ley N° 25.326, norma de orden público que regula los principios aplicables en la materia y el procedimiento de la acción de hábeas data. La Ley N° 25.326 ha sido reglamentada por el Decreto N° 1558/01, modificado mínimamente por su similar Decreto N° 1160/10.

Resumidamente, el objeto de la Ley N° 25.326 es la protección integral de los datos personales, asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados.

Dado que la Ley Nº 25.326 fue sancionada en octubre del 2000 y reglamentada un año después, resulta una obviedad destacar que los cambios de la tecnología operados en los últimos quince años han impactado en la protección de los datos personales y han surgido nuevas vulneraciones al derecho a la privacidad. En este mismo sentido, se debe recalcar el nuevo contexto internacional en la materia, particularmente las nuevas regulaciones en Europa que han sido recientemente aprobadas (Reglamento (UE) 2016/679) y que entrarán en vigencia en 2018.

Por estas razones, la DNPDP estimó conveniente iniciar en el presente año un proceso de reflexión sobre la necesidad de una reforma a la ley citada para contribuir al mejoramiento de la protección de los datos personales. Este proceso formó parte de la plataforma "Justicia 2020", un espacio de participación ciudadana e institucional para la elaboración, implementación y seguimiento de iniciativas y políticas de Estado, provisto por el Ministerio de Justicia y Derechos Humanos de la Nación.[1]

La DNPDP llevó adelante este proceso de reflexión convocando a actores interesados en la materia[2], provenientes del sector privado, del ámbito académico y de la sociedad civil, con quienes se realizó una serie de reuniones. Al momento de la elaboración de este documento ya se habían efectuado más de treinta reuniones, y se recibieron múltiples comentarios en aportes escritos y recolectados de la plataforma Justicia 2020.

El documento *Ley de Protección de los Datos Personales en Argentina (Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma-Agosto-Diciembre 2016)* que aquí se presenta, tiene como principal objeto el de constituirse en un insumo importante para encarar la redacción de las normas necesarias para mejorar la protección de los datos personales en Argentina, adaptándose a los nuevos tiempos y a la nueva normativa internacional.

Para llevar a cabo la redacción de un anteproyecto de ley, se consideró que resultaba mejor "primero escuchar y luego escribir". De allí la necesidad del proceso de

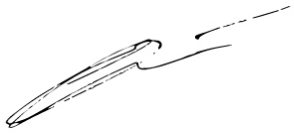
reflexión convocado. Asimismo, y para que las opiniones y sugerencias no quedaran únicamente en conocimiento de la DNPDP, se optó por compilarlas de una manera estructurada y por temas, a efectos de que puedan ser útiles para cualquiera de los interesados en proponer mejoras a la protección de los datos personales en Argentina. En otras palabras, este documento refleja las sugerencias y opiniones de los distintos actores que acudieron a la convocatoria de la DNPDP, aunque, claro está, no refleja ni debe ser entendido como opiniones o sugerencias de la DNPDP para su trabajo presente de interpretación de la normativa vigente ni para su trabajo en el futuro.

Por lo demás, y tal como fuera manifestado durante las reuniones, la DNPDP tiene previsto dentro de su planificación futura iniciar ese proceso de redacción de un anteproyecto de ley a fin de que, en caso de considerarse oportuno, el Poder Ejecutivo Nacional evalúe la pertinencia de su remisión como proyecto de ley al Congreso Nacional, y eventualmente, iniciar formalmente un proceso de reforma de la ley vigente. Este documento, además del objeto principal indicado anteriormente, tiene el propósito de convertirse en un instrumento útil tanto para contribuir en la agenda de las políticas públicas en estos temas, como para el trabajo que la DNPDP tiene previsto iniciar prontamente.

Cabe destacar que, si bien es cierto que la DNPDP está abierta a continuar recibiendo aportes a este proceso de reflexión, de manera directa o a través de la plataforma "Justicia 2020" durante 2017, no es menos cierto que con los materiales hasta ahora recogidos, sumado a la experiencia de la DNPDP, ya se está en condiciones de comenzar con el desarrollo del borrador del anteproyecto de ley señalado.

Finalmente, la DNPDP agradece sinceramente a todos aquéllos que aceptaron participar en el proceso de reflexión durante 2016. Se ha optado por mencionar de manera general a todos los que participaron del proceso al final de este documento, tanto personas como instituciones nacionales o extranjeras, y no realizar las identificaciones de los comentarios o sugerencias que aquí exponen con aquéllas.

Buenos Aires, 15 de diciembre de 2016



EDUARDO BERTONI
Director
Dirección Nacional de Protección de Datos Personales
Ministerio de Justicia y Derechos Humanos

RESUMEN EJECUTIVO

I. Acerca de la necesidad de la reforma de la Ley de Protección de Datos Personales en Argentina

- La opinión respecto a la necesidad de una reforma de la Ley de Protección de los Datos Personales (Ley Nº 25.326) fue prácticamente uniforme.

- En cambio, al discutirse acerca de la necesidad de una reforma parcial o una reforma total de la ley no hubo unanimidad. Algunos defendieron debería realizarse una reforma total, mientras que otros defendieron que lo más conveniente sería realizar una reforma parcial de la ley que permitiese a la Argentina mantener la mayoría de los reconocimientos y condiciones previamente obtenidos ante otros países.

- Varios de los participantes de las reuniones coincidieron en la necesidad de que la Ley Nº 25.326 se adecue al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, aunque también se sugirió a lo largo de las reuniones otros modelos a tomar de referencia; entre ellos, el APEC Privacy Framework y el APEC Cross Border Privacy Rules (CBPR) system, así como el Acuerdo Transpacífico de Cooperación Económica.

- En varias reuniones se enfatizó la idea de que el buen uso de los derechos en el ámbito de la protección de datos personales no es incompatible con la innovación.

II. Acerca de las disposiciones generales de una ley de protección de datos personales

Sobre el objeto de la ley

- Todos los actores que participaron de la serie de reuniones sobre la reforma de la Ley Nº 25.326 y que hicieron referencia a su objeto, coincidieron en que esa ley debiese incluir a todas las bases de datos –públicas o privadas- que realicen operaciones de tratamiento de datos personales.

Sobre el alcance de la ley

- Una amplia mayoría sostuvo que la Ley Nº 25.326 no debería proteger a las personas jurídicas, o al menos, no debería protegerlas en igual grado que a las personas físicas. Esta postura se condice con los estándares internacionales en la materia.

Sobre el ámbito de validez espacial de la ley

- Se propuso que la nueva legislación establezca su aplicabilidad a todo responsable que realice operaciones de tratamiento de datos de residentes en Argentina, aunque su sede, su base de datos o las operaciones de tratamiento no se encuentren o no se realicen en el país.

- Contrariamente a esta posición, también se propuso que se deberían aplicar las leyes según la sede o establecimiento principal del responsable de datos.

Sobre la jurisdicción y competencia

- Se sugirió analizar la posibilidad de prever que todos los asuntos referidos a archivos de datos interconectados en redes de alcance interjurisdiccional correspondieran a la justicia local (o al menos aquellos relacionados a bancos de datos de titularidad privada interconectados).
- Alternativamente, se sugirió que simplemente se deje a criterio del actor elegir la vía federal o local para efectuar su reclamo.

Sobre las definiciones en la ley

- Una minoría propuso que se incluyese expresamente a los metadatos como dato personal dentro de la Ley Nº 25.326.
- Hubo consenso en que la definición de datos sensibles debiera revisarse y ampliarse.
- Una reforma de la ley debiese, por un lado, revisar la definición de "disociación de datos", y por otro, contemplar qué procedimiento se debería seguir en caso de que un dato supuestamente disociado pasara a estar asociado a una persona nuevamente.
- Un gran número de actores recalcó, a título de comentario general, que habría que rever ciertos errores semánticos de la ley, unificar algunos términos y delimitar mejor ciertos términos vagos.

III. Acerca de los principios generales de una ley de protección de datos personales

Sobre la calidad de los datos

- Muchos de los actores que intervinieron en las reuniones recalcaron la necesidad de revisar el principio de calidad de los datos (en relación a la finalidad de los datos) tal como está previsto en la ley vigente.
- Se sugirió se incluya la posibilidad de que los datos objeto de tratamiento puedan ser tratados para finalidades diferentes a las que originalmente motivaron su obtención en la medida que no resulten contrarias.

Sobre el consentimiento

- El consentimiento fue un tema abordado en la mayoría de las reuniones.
- Muchos recalcaron la necesidad de flexibilizar el concepto de consentimiento que recepta la Ley Nº 25.326. Sustentaron su postura en que, en un mundo en el que se producen continuamente transacciones que implican tratamiento de datos personales cuando una persona utiliza servicios y productos en Internet, no es realista esperar que las personas deban recibir y procesar solicitudes de consentimiento para cada interacción que conlleve el uso de sus datos.
- Se estableció que la ley debiese permitir un consentimiento transparente pero implícito, sujeto al contexto en el cual un servicio sea utilizado, y restringir el

requerimiento de consentimiento explícito a situaciones específicas, donde por ejemplo se traten datos sensibles.

- Se sugirió se tomase como referencia el modelo mexicano y canadiense, marcos legales que reconocen que la forma de consentimiento necesaria para un tratamiento de datos concreto depende del contexto, admitiendo que el consentimiento tácito puede ser apropiado en circunstancias específicas y que no siempre es indispensable se dé por escrito.
- Varios propusieron se incluyera dentro de las excepciones al consentimiento la habilidad de procesar datos basados en intereses legítimos de las personas, siempre y cuando dichos intereses no se sobrepongan a la protección del individuo de sus derechos y libertades.

Sobre la seguridad de los datos

- En general se coincidió en que, tal como prevé el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, sería adecuado que la Ley Nº 25.326 contemplara la obligación de notificar la ocurrencia de un incidente de seguridad.
- No fue uniforme la opinión respecto a las condiciones de implementación de la mencionada obligación. Una mayoría coincidió en que no debería exigirse la notificación ante un incidente de seguridad en caso de que la amenaza de provocar un daño no fuese significativa.
- Varios destacaron sería conveniente que la Ley Nº 25.326 no estableciera un plazo determinado para efectuar las notificaciones de incidentes de seguridad. En este sentido, se sugirió que la ley disponga que se debe notificar "dentro de un plazo razonable" o "sin retrasos indebidos".

Sobre transferencia internacional de datos personales

- Fueron diversos los comentarios receptados en relación al flujo transfronterizo de datos personales.
- Varios actores indicaron sería conveniente se clarificaran los requerimientos que deben cumplir los acuerdos de transferencia internacional de datos.
- Algunos destacaron que la prohibición de la ley vigente que impide que se realicen transferencias internacionales de datos a terceros países específicos (países no adecuados) se opone a las tendencias existentes en la legislación de privacidad y al carácter global de muchos de los servicios de información actuales.
- A su vez, se recalcó sería imprescindible contemplar la situación especial de las transferencias internacionales de datos entre determinados sujetos (v. g. entre afiliados corporativos y entre responsables y encargados de datos). En estos casos, las transferencias probablemente entrarían dentro de las expectativas razonables del titular.
- Varios actores hablaron específicamente sobre la necesidad de regular el uso de cloud computing (o computación en la nube, como se lo denomina en español).

IV. Acerca de los derechos de los titulares de los datos personales

- En varias de las reuniones se sugirió la posibilidad de incluir algunos derechos de los titulares de los datos personales que actualmente no se encuentran contemplados en la Ley Nº 25.326.

Sobre el derecho de supresión (llamado "derecho al olvido")

- En relación a este tema, varios actores establecieron que la Constitución Nacional en su art. 43 y la Ley Nº 25.326 ya prevén una acción judicial específica para que los titulares de los datos personales puedan ejercer su derecho de supresión: la acción de hábeas data.
- Otros también sostuvieron que la facultad de ordenar se remuevan contenidos es exclusiva de la autoridad judicial, pero no sustentaron su posición en que la ley actual ya prevé un mecanismo para reclamar la supresión de datos personales, sino en que el derecho al olvido es un tema delicado que involucra un conflicto entre derechos de raigambre constitucional (libertad de expresión y derecho a la privacidad, el honor o la intimidad).
- Una minoría opinó que no habría inconveniente en que la autoridad de control pudiese ordenar la remoción de contenidos, siempre y cuando la ley estipulara precisamente en qué circunstancias podría ejercerse el derecho al olvido.

Sobre el derecho a la portabilidad de datos personales

- No hubo unanimidad en relación a la implementación del derecho a la portabilidad de los datos personales.
- Algunos destacaron que la portabilidad de los datos es técnicamente muy difícil de implementar, por lo que no debería incorporarse este derecho a la Ley Nº 25.326.
- Otros, en cambio, no advirtieron este problema. Sostuvieron que las personas deberían tener la posibilidad de solicitar y obtener todos los datos que proporcionaron a la organización en formato electrónico, en un período razonable de tiempo.

V. Acerca de las obligaciones de los responsables y encargados de tratamiento de datos personales

Sobre el registro de bases de datos personales

- Una mayoría propuso la eliminación del Registro Nacional de Bases de Datos y aquellos que sostuvieron que no habría inconveniente en que se siguiese exigiendo registración de las bases de datos, recalcaron se deberían adoptar ciertas modificaciones a esta obligación.

Sobre las normas de responsabilidad demostrada (*Accountability*)

- Hubo consenso generalizado en la necesidad de que se adopte un sistema de *accountability* (o normas de responsabilidad demostrada, en español). En este

sentido, se recomendó se tengan como referencia el APEC Cross Border Privacy Rules system[3] y el modelo mexicano de protección de datos personales[4].

Sobre un modelo basado en el riesgo

- Varios actores propusieron se incluya en la Ley Nº 25.326 el concepto de "enfoque basado en el riesgo", convirtiendo en responsabilidad de las organizaciones la evaluación del riesgo y el impacto del procesamiento de la información de los individuos y las acciones para mitigarlo.

Sobre el diseño desde la privacidad y por defecto (*Privacy by design – Privacy by default*)

- Algunos actores abordaron este tema, sugiriendo se implementen los principios de *privacy by design* y *privacy by default* en la Ley Nº 25.326.

Sobre la figura del Delegado de Protección de Datos Personales

- Muchos de los actores que intervinieron en el proceso de consulta apoyaron la inclusión de la figura del Delegado de Protección de Datos (en adelante "DPO"). Sin embargo, la mayoría planteó interrogantes a ser evaluados a la hora de adoptar su implementación.
- Varios participantes de las reuniones opinaron que es inviable que absolutamente todos los organismos estatales cuenten con un DPO.
- No hubo consenso en relación a las atribuciones que debería tener el DPO. Algunos opinaron que el DPO no sólo debería ser un interlocutor con la DNPDP sino también con los particulares. Mientras que otros sostuvieron que, de implementarse la figura del DPO, éste debería actuar exclusivamente como punto de contacto con la autoridad de control.

VI. Acerca de algunos supuestos especiales de tratamiento

Sobre el tratamiento de datos por organismos públicos

- Varios actores coincidieron en que la Ley Nº 25.326 le otorga al Estado demasiadas prerrogativas en lo que hace al manejo de datos personales de los particulares.

Sobre el tratamiento para servicios de información crediticia

- Aquellos actores que hicieron referencia a los servicios de información crediticia, coincidieron en que ciertas disposiciones de la ley vigente en relación a este tema debieran revisarse.
- Hubo disparidad de opiniones cuando se discutió sobre la posibilidad de prever la obligación por parte del acreedor de notificar al deudor antes de ceder información de incumplimientos patrimoniales a los bancos de datos que prestan servicios de información crediticia.

Sobre el tratamiento de grandes volúmenes de datos (*Big Data*)

Durante la serie de reuniones se hizo referencia a Big Data, sus implicancias en la actualidad y las discusiones y desafíos que plantea. Sin embargo, en general, no se recalcó la necesidad de incluir este concepto a la Ley Nº 25.326.

VII. Acerca de la autoridad de aplicación y control de la Ley de Protección de Datos Personales

Sobre el diseño institucional

- Todos los actores que hicieron referencia al órgano de control y su diseño institucional coincidieron en que sería necesario que la Ley Nº 25.326, de reformarse, contemplara una expansión de la capacidad de la DNPDP para cumplir con sus deberes de contralor.
- Para lograr este objetivo, se destacó que resultaría necesario aumentar la autonomía de la DNPDP y garantizar su adecuado financiamiento. Incluso, se sugirió se analizara la posibilidad de tener un órgano de control con capacidad presupuestaria propia.
- Se propusieron algunos mecanismos para reforzar la posición de la autoridad de control y dotarla de mayor autonomía.
- Vinculado con la reciente aprobación de la Ley de Acceso a La Información Pública (Ley Nº 27.275) se planteó la posibilidad de que fuese la misma autoridad la que aplicase las dos normativas, en lugar de tener dos entidades administrativas diferentes, así como sucede en otros países.

Sobre las sanciones que aplica la autoridad de aplicación

- Muchos actores reconocieron sería necesaria una revisión y actualización de las sanciones vigentes.
- Se advirtió, sin embargo, que de establecer un mecanismo de actualización automática del monto de las multas, fijar las ganancias del infractor como un valor de referencia sería problemático para muchas industrias e incluso injusto. Como regla, las sanciones deben ser proporcionales al daño y no a las ganancias del infractor.
- Por otro lado, un sector estableció que la cancelación de las bases de datos o el bloqueo de sitios web no sería una sanción administrativa válida.

I. ACERCA DE LA NECESIDAD DE LA REFORMA DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN ARGENTINA

La opinión respecto a la necesidad de una reforma de la Ley Nº 25.326[5] fue uniforme, a excepción del sector de marketing que destacó que, desde su ámbito, no sería necesaria ninguna modificación sustancial. Sin embargo, incluso este sector no vio ningún inconveniente en que se reformara la ley vigente siempre y cuando se tomasen los reparos para que la Argentina pudiese seguir siendo considerada un país con nivel de protección adecuado por la Unión Europea[6].

En cambio, al discutirse acerca de la necesidad de una reforma parcial o una reforma total de la ley no hubo unanimidad. Algunos defendieron debería realizarse una reforma total, empezando de cero. Para sustentar esta postura, un actor utilizó una comparación: ***la Ley Nº 25.326 funciona como una bicicleta. El problema de la bicicleta es que no se le puede agregar alas para volar. En una era en la que es indispensable volar por el continuo cambio que se produce en el ámbito de la tecnología se necesita una ley que funcione como un jet.***

Otros defendieron que lo más conveniente sería realizar una reforma parcial de la ley que permitiese a la Argentina mantener la mayoría de los reconocimientos y condiciones previamente obtenidos ante otros países, a la vez que adecuarse a la nueva realidad social y relaciones personales que se habrían desarrollado con el uso de las nuevas tecnologías. Además, se advirtió acerca de los riesgos que podrían derivarse de cambiar absolutamente todas las reglas de juego.

Por otro lado, los participantes de las reuniones coincidieron en la necesidad de que la Ley Nº 25.326 se adecuara al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante "Reglamento (UE) 2016/679")[7], para que Argentina siguiese siendo un país con nivel de protección adecuado conforme los lineamientos europeos y, por ende, continuara teniendo una ventaja comparativa en el mercado en relación a otros países con un nivel de protección no adecuado. Algunos, sin embargo, advirtieron sobre el potencial riesgo de importar integralmente todas las disposiciones del Reglamento (UE) 2016/679 a la Ley Nº 25.326, puesto que al no haber sido todavía implementado en Europa (el Reglamento (UE) 2016/679 será aplicable a partir del 25 de mayo de 2018) no se habrían puesto a prueba algunos institutos nuevos cuya efectividad habría sido cuestionada por académicos y estudiosos de la materia (v. g. la portabilidad de los datos). Por este motivo, este grupo sugirió se tuviese sumo cuidado al momento de analizar qué disposiciones y nuevas figuras adoptadas por el Reglamento sería conveniente receptar en la Ley Nº 25.326.

Además de indicar se tuviera en cuenta el Reglamento (UE) 2016/679 como modelo para una eventual reforma, también se sugirieron a lo largo de las reuniones otros modelos a tomar de referencia; entre ellos, el APEC Privacy Framework[8] y el APEC Cross Border Privacy Rules (CBPR) system[9], así como el Acuerdo Transpacífico de Cooperación Económica[10]. Un sector muy minoritario recomendó también tener en cuenta el informe del Comité Jurídico Interamericano, titulado "Privacidad y protección de datos personales" de 2015[11].

Asimismo, en algunas reuniones se sugirió se podría rever el proceso de hábeas data tal como está regulado en la ley vigente. Así, por ejemplo, se destacó la ley debiese contemplar mecanismos para agilizar el proceso de hábeas data, protegiendo de esta manera al titular de los datos. Específicamente, se hizo énfasis en que la ley debiese permitir un control judicial *ex post* pero no *ex ante*, exigiendo siempre se presentaran inicialmente los reclamos en la órbita administrativa (en la DNPDP, que es la autoridad competente en la materia). Opinaron que ésta sería una manera de lograr se agilizara el proceso de hábeas data.

Por último, cabe destacar algunos comentarios generales que se presentaron en relación a una potencial reforma. En primer lugar, se enfatizó la idea de que el buen uso de los derechos en el ámbito de protección de datos personales no es incompatible con la innovación, como algunos erróneamente creen.

En segundo lugar, se recalcó que la Ley Nº 25.326 debiera buscar igualar o mejorar las condiciones de residir en Argentina respecto de residir en el exterior, evitando transformarse en una limitación para los que se encontraran dentro del país y que fuese eludida por los que se situaran fuera.

Particularmente, se sugirió que se adoptara el principio de "prohibición por excepción" en la ley, en lugar del principio de "libertad por excepción". Se opinó que se debería poder hacer todo lo que no se prohíbe y no solamente aquello que se permite. Así por ejemplo, se indicó que la Ley Nº 25.326 aplica la "libertad por excepción" cuando exige consentimiento previo para cualquier dato a excepción de: nombre, documento nacional de identidad, identificación tributaria y previsional, ocupación, fecha de nacimiento y domicilio. Debiera adoptarse la "excepción por prohibición" para evitar excluir al interesado del acceso a la innovación.

Finalmente, se compartió sería conveniente que la ley incluyera en determinadas situaciones instancias de conciliación o mediación previas a la imposición de una sanción a la parte incumplidora, tal como contempla la Ley Nº 24.240[12]. Asimismo, se propuso se revisaran los plazos contemplados en la ley vigente. En este sentido, se estableció que así como el Código Civil y Comercial de la Nación[13] ha tendido a reducir los plazos de prescripción, la Ley Nº 25.326, pese a no contemplar exactamente plazos de prescripción sino de caducidad, también debería reducirlos para estar más acorde con las directrices del Código.

II. ACERCA DE LAS DISPOSICIONES GENERALES DE UNA LEY DE PROTECCIÓN DE DATOS PERSONALES

Sobre el objeto de la ley

Todos los actores que participaron de la serie de reuniones sobre la reforma de la Ley Nº 25.326 y que hicieron referencia a su objeto, coincidieron en que esa ley debiese incluir a todas las bases de datos –públicas o privadas- que realicen operaciones de tratamiento de datos personales. Por ello, sostuvieron que ***debería revisarse la actual redacción, que establece que la ley tiene como objeto las bases de datos privadas "destinadas a dar informes", ya que causa una indebida***

restricción a su ámbito de aplicación. De tal suerte, la opinión fue unánime en torno a que la expresión de "destinadas a dar informes" debiese ser eliminada.

Uno de los actores sugirió que la ley, en lugar de referirse a bases privadas destinadas a dar informes, debería referirse específicamente a bases con datos personales cuyo objeto fuese exteriorizar esos datos personales a terceros ajenos al responsable de la base de datos, y fuera del cumplimiento de obligaciones legales/fiscales o que se utilizasen para la ejecución de otras operaciones.

En este sentido, destacó que debieran excluirse del objeto de la ley aquellas bases que usualmente se utilizan "hacia adentro" (v. g. clientes, personal, proveedores, administración, backup, gestión, entre otros), como así las utilizadas en procedimientos automatizados (telecomunicaciones en general, ruteos, procesamientos y transmisión de emails, o hosting, backups remotos, entre otros). Asimismo, sostuvo que deberían excluirse las exteriorizaciones que se realizasen en cumplimiento de otras leyes, como informes a las autoridades fiscales o a la seguridad social, ya que no son el objeto de cualquier exteriorización sino de unas específicas, restringidas, y reguladas por esas otras leyes.

Sobre el alcance de la ley

Una amplia mayoría sostuvo que la Ley Nº 25.326 no debería proteger a las personas jurídicas, o al menos, no debería protegerlas en igual grado que a las personas físicas. Esta postura se condice con los estándares internacionales en la materia.

Así, a título de ejemplo, se puede destacar la opinión de uno de los actores que sugirió se tuviesen en cuenta las pautas elaboradas por el Sistema Interamericano de Derechos Humanos. En este sentido, la Opinión Consultiva OC-22/16[14] establece que las personas jurídicas no son titulares de los derechos establecidos en la Convención Americana de Derechos Humanos (cons. 70). Considerando que el derecho a la protección de los datos personales posee un fuerte vínculo con el resguardo a la privacidad, la intimidad y la honra de las personas (derechos establecidos en la Convención Americana de Derechos Humanos) la mayoría de las garantías y derechos sólo deberían aplicarse a las personas físicas. Esto no implica reconocer que no existan casos en los que una persona jurídica pueda necesitar la protección de sus datos (v.g. el caso de que una empresa figure incorrectamente como morosa en una base de datos). Sin embargo, estos casos de excepción deberían ser establecidos explícitamente en la ley, a fin de evitar que ciertos derechos que corresponden a personas físicas sean utilizados de manera incorrecta por personas jurídicas.

Sobre el ámbito de validez espacial de la ley

Un actor se refirió al fenómeno digital que ha provocado no existan límites geográficos en materia de operaciones de tratamiento de datos. En virtud de esto, los datos de los ciudadanos argentinos han sido y son a diario objeto de tratamiento por parte de entidades cuya sede no se encuentra en territorio argentino, cuyas bases de datos no se encuentran en el país o cuyas operaciones de tratamiento se realizan en el extranjero. Es por ello que se propuso que la nueva legislación establezca su aplicabilidad a todo responsable que realice operaciones de

tratamiento de datos de residentes en Argentina, aunque su sede, su base de datos o las operaciones de tratamiento no se encuentren o no se realicen en el país.

Contrariamente a esta posición, otro participante de las reuniones determinó sería positivo para los consumidores que las autoridades nacionales intentaran armonizar las leyes de protección de datos, ofreciendo medidas de protección internacionales significativas, equilibradas y coherentes que permitieran a las empresas operar en un entorno predecible en el que se cumplieran las regulaciones. Según destacó, la mejor manera de cumplir este objetivo sería utilizar leyes que se aplicaran según la sede o establecimiento principal del responsable de datos. Así, en lugar de conllevar acciones en un país que podrían perjudicar los esfuerzos de otras autoridades nacionales de protección de datos, un marco jurisdiccional en el que el regulador de la sede principal de la entidad pudiese coordinar las investigaciones colaborando con otros reguladores cuyos integrantes estuviesen afectados podría provocar cambios más amplios a escala mundial y, a su vez, fomentar una mayor predictibilidad para las entidades reguladas.

Sobre la jurisdicción y competencia

Un sector hizo énfasis en los problemas de competencia judicial que se derivan de la Ley Nº 25.326 y su aplicación.

De efectuarse una lectura compatible de los arts. 36 y 44 de la Ley Nº 25.326[15] (se indicó que hay un sector de la doctrina que expresa habría una contradicción entre ambos artículos) se extrae que corresponde a los juzgados federales intervenir en las demandas articuladas contra bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional, sean éstos de titularidad pública o privada, y se trate o no de un hábeas data.

Bajo este escenario, se expresó que, de considerar que la competencia federal fuese en razón de las personas, la competencia respecto de los juicios iniciados por o contra los bancos de datos de titularidad privada interconectados en redes de alcance interjurisdiccional podría ser prorrogable.

Sin embargo, se destacó que, conforme la interpretación de la Corte Suprema de Justicia de la Nación[16], cuando el art. 36 párr. 2 inc. b) de la ley dispone que intervendrán los juzgados federales en los procesos que involucren archivos de datos que se encuentren interconectados en redes de alcance interjurisdiccional, establece una pauta de atribución de competencia por la materia (entendiendo que las redes interjurisdiccionales estarían captadas por la cláusula comercial de la Constitución Nacional –art. 75 inc. 13-, concerniente a la regulación del tráfico interprovincial o internacional).

A raíz de esta interpretación de la Corte, aquellas demandas que se interponen contra bases de datos de titularidad privada interconectadas no pueden ser prorrogables y atendidas por la justicia local, derivando en graves afectaciones contra los derechos de los afectados. La asignación de un juez distante para aquellos que residen a considerables distancias de tribunales federales se convierte en un serio obstáculo en el ejercicio de una acción que debiese ser expedita, rápida y eficaz.

Por estos motivos, ***se sugirió se analizara la posibilidad de prever que todos los asuntos referidos a archivos de datos interconectados en redes de alcance interjurisdiccional correspondieran a la justicia local (o al menos aquellos relacionados a bancos de datos de titularidad privada interconectados).*** Alternativamente, se sugirió que simplemente se dejara a criterio del actor elegir la vía federal o local para efectuar su reclamo.

Sobre las definiciones en la ley

- **Metadatos**

Una minoría propuso que se incluyese expresamente a los metadatos como dato personal dentro de la Ley Nº 25.326. Se define comúnmente a los metadatos como datos sobre datos, es decir información estructurada que describe a otra información. La importancia de los metadatos radica en que permiten revelar tanto o más acerca de las personas que el propio contenido de las comunicaciones, ya que a través de ellos se pueden establecer patrones de comportamiento, hábitos o relaciones.

- **Datos sensibles**

Hubo consenso en que la definición de datos sensibles debiera revisarse y ampliarse.

Algunos sugirieron que extender la definición por enumeración no sería la forma más adecuada de contemplar supuestos nuevos que pueden calificar como datos sensibles, dado que se correría el riesgo de que esa definición quedara desactualizada al poco tiempo. En este sentido, se sugirió se incluyese dentro de la definición de dato sensible la frase "o cualquier dato personal cuyo uso pudiese ser potencialmente discriminatorio" y de esta manera, lograr una fórmula que se pudiese extender en el tiempo.

Otros, en cambio, no advirtieron sobre el potencial riesgo de ampliar la definición por enumeración y sugirieron se contemplase expresamente a los datos genéticos y biométricos, en tanto estén dirigidos a identificar de manera unívoca a una persona física. También un grupo defendió la inclusión de los datos relativos a la orientación sexual.

Una minoría puntualizó que no necesariamente todos los datos biométricos que identifican a una persona deberían ser considerados datos sensibles, sino exclusivamente aquellos que pudiesen revelar algunos datos adicionales cuyo uso pudiese ser potencialmente discriminatorio (v.g. datos que revelasen origen étnico o información referente a la salud, y no así una mera huella dactilar).

- **Disociación de datos**

La Ley Nº 25.326 define a la "disociación de datos" como "todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable". A raíz de este concepto, ha surgido una discusión en el

mundo de la tecnología en torno a si verdaderamente existe un procedimiento de anonimización real de los datos personales en el que efectivamente concurra una verdadera disociación de los datos, que de ninguna manera permita relacionar los datos con una persona identificada o identificable.

En relación a esta discusión, ***un sector negó la posibilidad de lograr una verdadera anonimización de los datos, puesto que cualquier dato disociado puede volver a asociarse.*** Destacaron que es muy difícil técnicamente que una vez disociado el dato no se pueda volver atrás. Por esta razón, establecieron que una reforma de la ley debiese, por un lado, revisar la definición de "disociación de datos", y por otro, contemplar qué procedimiento se debería seguir en caso de que un dato supuestamente disociado pasara a estar asociado a una persona nuevamente.

- **Otros términos**

Un gran número de actores recalcó, a título de comentario general, que habría que rever ciertos errores semánticos de la ley, unificar algunos términos (v. g. archivo, registro, base, banco de datos) y delimitar mejor ciertos términos vagos (v. g. "de acuerdo a las circunstancias", "en cuanto resulte pertinente").

Algunos, a su vez, establecieron se debería rever la definición de "dato personal" pero sin sugerencias respecto a qué modificaciones deberían llevarse a cabo.

Por último, un actor advirtió sobre el riesgo en el que se está incurriendo actualmente al extender la aplicación de la Ley Nº 25.326 a áreas que no son necesariamente una base de datos personales, resultando pernicioso muchas veces para el derecho a la libertad de expresión. Por este motivo, recalcó la importancia de limitar el alcance de la Ley Nº 25.326, definiendo adecuadamente "dato personal", "base de datos personales", "responsable de tratamiento" y "encargado de tratamiento". Conforme su opinión, se podría definir al "responsable de tratamiento" como una persona física o jurídica, titular de la base de datos, que decide sobre la finalidad de los datos, y al "encargado de tratamiento" como un tercero que por cuenta y nombre del responsable llevara a cabo cualquier tratamiento de datos personales. Sugirió se tuviese en cuenta las definiciones brindadas por la legislación de Canadá[17] y Singapur[18].

III. ACERCA DE LOS PRINCIPIOS GENERALES DE UNA LEY DE PROTECCIÓN DE DATOS PERSONALES

Sobre la calidad de los datos

Muchos de los actores que intervinieron en las reuniones recalcaron la necesidad de revisar el principio de calidad de los datos (en relación a la finalidad de los datos) tal como está previsto en la ley vigente.

Un sector indicó que la redacción del art. 4 inc. 3 de la Ley Nº 25.326 que establece: "[l]os datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención" es ambigua y presta a confusión. Según se opinó, la acepción del término "incompatibles" es muy amplia,

difusa y depende de la subjetividad de quien interpreta. Por otro lado, destacaron que en general es imposible evitar usos estrictamente "distintos" a los ideados originalmente. De interpretarse el término "distintas" en forma estricta, se limitan exageradamente los usos de la información haciéndoles perder valor y resultando inconveniente para el propio titular de los datos.

Por este motivo, ***se sugirió se incluya la posibilidad de que los datos objeto de tratamiento puedan ser tratados para finalidades diferentes a las que originalmente motivaron su obtención en la medida que no resulten contrarias a éstas y, un actor agregó, siempre y cuando estas finalidades no sean perjudiciales para el titular de los datos.***

A su vez, en relación a este tema, varios actores sostuvieron que la Ley Nº 25.326 debería resolver la situación de una organización que recolecta datos personales para un propósito determinado y desea utilizarlos para un propósito distinto dentro de esa misma organización (sea que se utilicen internamente dentro de la compañía pero por otro sector/equipo que aquel que recolectó los datos o que se utilice por otra compañía dentro del mismo grupo económico).

Sobre el consentimiento

Fueron varias las discusiones que surgieron en relación al principio del consentimiento.

En primer lugar, distintos sectores advirtieron sobre la necesidad de modificar el art. 5 inc. 1 de la Ley Nº 25.326 en cuanto refiere a los medios mediante los cuales el titular de los datos puede prestar su consentimiento. Bajo la ley vigente, el consentimiento debe constar "por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias". Según expresaron, sería conveniente eliminar cierta ambigüedad al respecto, incluyendo a los medios electrónicos como medios idóneos para prestar consentimiento (v. g. aceptación electrónica, firma ***electrónica, firma digital, firma digitalizada).***

En segundo lugar, ***muchos recalcaron la necesidad de flexibilizar el concepto de consentimiento que recepta la Ley Nº 25.326. Sustentaron su postura en que, en un mundo en el que se producen continuamente transacciones que implican tratamiento de datos personales cuando una persona utiliza servicios y productos en Internet, no es realista esperar que las personas deban recibir y procesar solicitudes de consentimiento para cada interacción que conlleve el uso de sus datos.***

Se estableció que la ley debiese permitir un consentimiento transparente pero implícito, sujeto al contexto en el cual un servicio sea utilizado, y restringir el requerimiento de consentimiento explícito a situaciones específicas, donde por ejemplo se traten datos sensibles.

En esta misma línea, se destacó que el marco legal sobre protección de datos personales debiera contar con normas básicas bien razonadas que fuesen coherentes con las expectativas lógicas de las personas. Se debiesen reservar los procesos más formales de notificación y solicitud de consentimiento para esas situaciones en las que el tratamiento de datos fuera a diferir considerablemente de lo que cabría

esperar en la situación correspondiente o para esos casos en los que pudiese tener una repercusión material en el interesado.

En una de las reuniones se sugirió se tomase como referencia el modelo mexicano[19] y canadiense[20], marcos legales que reconocen que la forma de consentimiento necesaria para un tratamiento de datos concreto depende del contexto, admitiendo que el consentimiento tácito puede ser apropiado en circunstancias específicas y que no siempre es indispensable se dé por escrito.

En tercer lugar, varios hicieron referencia a las situaciones en las que es innecesario el consentimiento del titular para el tratamiento de sus datos. Sugirieron se modificasen algunas de estas excepciones receptadas en el art. 5 inc. 2 de la Ley Nº 25.326.

Por un lado, se destacó sería necesario revisar el apartado (c) del art. 5 inc. 2, que establece que no será necesario el consentimiento del titular cuando: "[s]e trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio". En esta disposición propusieron se incorporara el domicilio electrónico, el teléfono y el celular.

En relación a esto, un sector recalcó que la excepción debiese contemplar a todos los nuevos "domicilios" de la actualidad y los posibles a futuro. Indicaron que actualmente casi cualquier titular de datos pasa mucho más tiempo en su "domicilio virtual" (red social, email, mensajería, etc.) que en su "domicilio-casa", por lo que en la práctica ya habría sido sobrepasada aquella vieja idea de domicilio, según la cual sería el "domicilio-casa" la única circunscripción territorial donde se asienta una persona para ejercer sus derechos y cumplir sus obligaciones. Bajo este criterio, se propuso ampliar el rango de ubicaciones del titular, eliminando el término "domicilio" y agregando en vez: "*y otros datos de contacto del Titular, como: domicilio, domicilio electrónico, email, mensajerías, direcciones de red, identificadores, teléfono, celular, y los que se utilicen a tal efecto.*"

Por otro lado, un grupo sugirió se revisara el apartado (d) del art. 5 inc. 2, que prevé la excepción al consentimiento para aquellos datos personales que "[d]eriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento".

Un sector indicó que, de la manera en la que está escrito el apartado, no se entiende si la excepción es para aquellos datos que deriven de una *relación contractual o científica o profesional*, o si en cambio, es para aquellos que deriven de una *relación contractual científica o de una relación contractual profesional*. Defendieron que esto debería aclararse.

Otro sector no advirtió aquel problema, sino estableció que la Ley Nº 25.326 al incluir la noción del tratamiento de datos en el cumplimiento de una relación contractual como una excepción del requisito de consentimiento, pero limitándolo a una relación contractual "científica o profesional", estaría dejando afuera otras formas que pueden adoptar las relaciones contractuales o transaccionales que son esenciales para el funcionamiento eficaz de las sociedades digitales. De tal suerte, se sugirió se tomara de referencia el Reglamento (UE) 2016/679[21], que admite que las acciones

que se lleven a cabo para cumplir un contrato (sin distinción) proporcionen una base legal para justificar el tratamiento de datos.

Asimismo, varios propusieron se incluyera dentro de las excepciones al consentimiento la habilidad de procesar datos basados en intereses legítimos de las personas, siempre y cuando dichos intereses no se sobrepongan a la protección del individuo de sus derechos y libertades. El interés legítimo ofrece flexibilidad para innovar y para implementar medidas antifraude y de seguridad más sofisticadas. Al igual que con el punto anterior, se aconsejó se tomara como modelo el Reglamento (UE) 2016/679[22].

Por último, fueron varias las opiniones que surgieron en relación al consentimiento de los niños y adolescentes.

Un actor determinó no sería deseable que la Ley Nº 25.326 impusiera requisitos de consentimiento estricto por parte de los padres para que los adolescentes pudiesen utilizar servicios en Internet. Estableció que, dado que en la actualidad la tendencia de tener dispositivos personales para cada miembro de la familia va en aumento, las oportunidades para que los padres den su consentimiento son más escasas. Esto hace que los adolescentes puedan perderse cada vez más cantidad de información y experiencias valiosas o que mientan sobre sus edades para tener acceso a estos contenidos. Además, opinó que la necesidad de que los padres tengan que dar su consentimiento para el tratamiento de los datos de los adolescentes podría desalentar el desarrollo de contenidos y servicios beneficiosos dirigidos a los más jóvenes. Por estos motivos, se expresó sería mejor que, en lugar de imponer políticas de consentimiento estricto para los adolescentes, la autoridad de control pudiese trabajar para garantizar que los servicios en Internet ofrecieran herramientas para enseñar tanto a los padres como a los más jóvenes y ayudarlos a tomar buenas decisiones en torno a la privacidad y seguridad de sus datos.

Otro actor, en cambio, hizo mención a la edad a partir de la cual debiera considerarse válido el consentimiento otorgado por un menor para el tratamiento de sus datos personales. Así expresó que, por regla general, el consentimiento debería considerarse válido a partir de los 13 años de edad, tal como se admite en la práctica en Estados Unidos. Dicha regla también podría extraerse del Reglamento (UE) 2016/679, puesto que si bien requiere el consentimiento del titular de la patria potestad para menores de 16 años, permite a los Estados miembros establecer por ley una edad inferior a tales fines, siempre que no sea inferior a 13 años[23]. Según su opinión, de establecer la edad mínima en 16 años, se podría correr el riesgo de dejar afuera del uso de Internet a algunos jóvenes adultos. De todas formas, se enfatizó que el consentimiento del titular de la patria potestad para el tratamiento de datos personales del menor de edad a su cargo no sería necesario en situaciones donde el tratamiento se requiriera para dar cumplimiento a una obligación legal o en situaciones donde corriese riesgo la integridad física de la persona.

Finalmente, y en relación a este tema, se aconsejó revisar qué establece el Código Civil y Comercial de la Nación al respecto, así como el Reglamento (UE) 2016/679 y la ley colombiana de protección de datos personales (Ley Estatutaria No. 1581)[24]. Específicamente, un sector consideró se debería receptar acabadamente lo establecido por el Reglamento (UE) 2016/679 en lo atinente a este punto, a excepción del inc. 2 del art. 8, que propuso modificar según: *"El responsable del tratamiento hará los mejores esfuerzos que considere razonables para verificar en*

tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta sus posibilidades para hacerlo."

Sobre la seguridad de los datos

En general se coincidió en que, tal como prevé el Reglamento (UE) 2016/679, sería adecuado que la Ley Nº 25.326 contemplara la obligación de notificar la ocurrencia de un incidente de seguridad[25]. Algunos, sin embargo, se apartaron de los lineamientos del Reglamento, sugiriendo se notifique al afectado además de a la autoridad de control.

No fue uniforme la opinión respecto a las condiciones de implementación de la mencionada obligación. Una mayoría coincidió en que debería exigirse la notificación ante un incidente de seguridad sólo en caso de que la amenaza de provocar un daño fuese significativa. De lo contrario, se sostuvo se correría el riesgo de caer en rigorismos formales absurdos, logrando que los titulares de los datos ni prestasen atención a esas notificaciones. A su vez, se abrumaría a la DNPDP de notificaciones, impidiendo se avocara a casos donde realmente ameritase su intervención, esto es, casos de efectivo daño material. En este sentido, se podría tomar el Reglamento (UE) 2016/679 como referencia, en tanto excluye la necesidad de notificación cuando sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y las libertades de las personas.

Un actor agregó al requisito anterior una condición adicional: la filtración de datos provocada por el incidente de seguridad debería afectar a una gran cantidad de titulares para que se activara la obligación de reportar (v. g. en Estados Unidos muchos estados imponen un límite mínimo de 500 personas[26] para que los reguladores encargados de la seguridad de los consumidores puedan centrarse únicamente en filtraciones de gran repercusión). Además, añadió que se debiese incluir una excepción para filtraciones de datos cifrados o datos que, de alguna forma, fuesen inservibles para la persona no autorizada, donde el afectado no corre riesgo alguno.

Otro participante opinó que, dentro del ámbito privado, se debería hacer una distinción entre las sociedades que cotizan en bolsa y aquellas sociedades que no, e imponerles únicamente a estas últimas la obligación de notificar al órgano de control frente a un incidente de seguridad.

Su argumento fue pragmático: las empresas "chicas" (como denominó, en términos generales, a las sociedades que no cotizan en bolsa) generalmente hacen un análisis costo-beneficio, evaluando el costo que les implicaría adoptar todas las medidas de seguridad que exige la Ley Nº 25.326 y sus reglamentaciones y el costo que sufrirían en caso de ser sancionadas por no adoptar los mecanismos pertinentes de seguridad. Al hacer este análisis, la mayoría de las veces las empresas chicas terminan prefiriendo no adoptar medidas de seguridad y eventualmente pagar la multa en caso de que les recaiga una inspección. En cambio, las empresas "grandes" (tomando como referencia a las sociedades que cotizan en bolsa) suelen tomar todas las medidas de seguridad que la Ley Nº 25.326 impone e incluso medidas adicionales que no exige la ley. Esto se debe a que tienen controles externos periódicamente, por lo que suelen no tener opción de cumplir con los requerimientos

debidos, además de que los costos reputacionales de no contar con un estándar razonable de seguridad son muy elevados.

De tal suerte, sugirió tendría sentido exigir a las sociedades que no cotizan en bolsa que notifiquen a la autoridad de control frente a un incidente de seguridad porque probablemente podría contribuir a acotar el riesgo. No así en el caso de sociedades que cotizan en bolsa, donde imponerles la obligación de notificar al órgano de control frente a estas situaciones les significa una mera formalidad, puesto que las empresas ya tienen medidas de seguridad implementadas y cuentan con un equipo de trabajo para resolver este tipo de cuestiones de la manera más eficiente.

Por otro lado, varios destacaron sería conveniente que la Ley Nº 25.326 no estableciera un plazo determinado para efectuar las notificaciones de incidentes de seguridad. En este sentido, se sugirió que la ley disponga que se debe notificar "dentro de un plazo razonable" o "sin retrasos indebidos". De esta manera, se evitaría que el responsable de tratamiento no tuviera tiempo suficiente para encontrar la causa del incidente de seguridad y pudiese averiguar adecuadamente qué es lo que habría sucedido. Así, por ejemplo, algunas leyes estatales de Estados Unidos prevén el retraso de la notificación ante incidentes de seguridad por motivos justificados[27]. Asimismo, el Reglamento (UE) 2016/679, pese a estipular un plazo determinado, también deja abierta la posibilidad de extender el plazo con debida justificación.

Por último, se brindaron algunos comentarios generales concernientes a los requerimientos de seguridad y al rol de inspección llevado a cabo por la DNPDP. Algunos participantes de las reuniones hicieron aportes en vistas de una posible modificación a la Disposición 11/2006, referida a medidas de seguridad. Entre otras sugerencias, se mencionó se podría utilizar la Estrategia de Ciberseguridad Nacional Española de 2013[28] como modelo. Adicionalmente, se advirtió sobre la importancia de mantener los requerimientos de seguridad en la capa más general, puesto que con el ritmo de desarrollo constante y rápido de la tecnología, los requerimientos regulatorios excesivos podrían convertirse velozmente en obsoletos.

Sobre el deber de confidencialidad

Sólo algunos actores abordaron el tema referido al deber de confidencialidad.

En primer lugar, se mencionó que si bien el apartado del art. 10 de la Ley Nº 25.326 refiere a "deber de confidencialidad", en los incisos se alude a "secreto profesional". Tendría sentido unificar los términos, refiriendo exclusivamente al deber de confidencialidad.

En segundo lugar, varios recalcaron la necesidad de revisar el art. 10 inc. 2 de la Ley Nº 25.326, que trae aparejadas algunas dificultades al momento de su aplicación. Conforme esta disposición, "el obligado [a mantener confidencialidad] podrá ser relevado del deber de secreto profesional por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública". Estas razones que la ley le brinda a los jueces para autorizar se releve del deber de confidencialidad han demostrado ser en la práctica muy restrictivas. Los jueces suelen no fundar el relevamiento del deber de confidencialidad en estas tres razones, sino en otros motivos (o incluso sin justificación alguna). Esto hace que a los responsables de la base de datos se les presente una disyuntiva: cumplir con la ley o

cumplir con la orden judicial. Por este motivo, se sugirió contemplar razones adicionales para relevar al responsable de la base de datos de su obligación de mantener la confidencialidad de los datos, a lo mejor remitiendo a otras normativas.

Finalmente, se advirtió sobre otro problema que se da comúnmente en la práctica: los organismos públicos suelen requerir información a los responsables de bases de datos, exigiendo se releve del deber de confidencialidad, aun sin que medie una ley o una orden judicial que autorice el acceso a los datos respectivos. Para evitar esto, se sugirió se incluya en la ley el principio rector según el cual se prohíbe a los organismos públicos el acceso a los datos personales sin mediar una ley o una orden judicial que lo permita expresamente.

Sobre transferencia internacional de datos personales

Fueron diversos los comentarios receptados en relación al flujo transfronterizo de datos personales.

Varios actores indicaron ***sería conveniente se clarificaran los requerimientos que deben cumplir los acuerdos de transferencia internacional de datos.*** No solo se advirtió sobre cierta vaguedad en la regulación de esta materia sino que se opinó habría una contradicción en los términos previstos en la Ley Nº 25.326 y en el Decreto Nº 1558/2001. En este sentido, sugirieron se trasladara a la Ley Nº 25.326 la excepción del consentimiento del titular a la prohibición de transferencia internacional de datos a países que no cuenten con un nivel de protección adecuado, que hoy está prevista exclusivamente en el Decreto Nº 1558/2001.

Adicionalmente, algunos destacaron que la prohibición de la ley vigente que impide que se realicen transferencias internacionales de datos a terceros países específicos (países no adecuados) se opone a las tendencias existentes en la legislación de privacidad y al carácter global de muchos de los servicios de información actuales. Para evitar perjudicar a los servicios de información, muchas legislaciones actuales de protección de datos que imponen limitaciones en las transferencias autorizan éstas a nivel internacional en aquellos casos en los que una empresa puede proporcionar una protección adecuada de la privacidad.[29] De esta manera, además de reconocer el consentimiento como la base de cualquier transferencia, se pueden tener en cuenta normas vinculantes corporativas y cláusulas contractuales que requieran que los receptores de los datos asuman las mismas obligaciones ante el titular de los datos que fueron asumidas por el responsable que los transfirió.

En relación a este punto, se estableció que, en principio las transferencias deberían ser permitidas, asegurando siempre que el individuo responsable en Argentina permaneciera como tal y fuese pasible de asumir esa responsabilidad, fuesen los datos procesados localmente o en otro país. A su vez, debería asegurarse que el destinatario proveyera el nivel correcto de seguridad.

Un participante agregó a esta discusión que sería ideal se evitaran los pedidos de permisos previos a la transferencia de información. Según su opinión, cualquier requerimiento *ex-ante* tendría el potencial de impedir la innovación y de convertirse en obsoleto en la práctica. Debería ser suficiente tener la posibilidad de asegurar el cumplimiento de la ley entre las partes involucradas.

A su vez, se recalcó sería imprescindible contemplar la situación especial de las transferencias internacionales de datos entre determinados sujetos (v. g. entre afiliados corporativos y entre responsables y encargados de datos). En estos casos, las transferencias probablemente entrarían dentro de las expectativas razonables del titular. Por lo tanto, en principio, los requisitos de consentimiento estricto por adelantado no serían necesarias para proteger la privacidad de los datos del titular, especialmente cuando el receptor estuviese obligado a respetar las mismas obligaciones de privacidad a aquellas asumidas por el responsable que habría transferido los datos.

En este sentido, se sugirió se tomara de referencia el modelo mexicano, que parecería haberse basado en las consideraciones precedentes para plantear el enfoque del artículo 37 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[30]. Éste permite la transferencia nacional o internacional de datos sin necesidad de obtener el consentimiento del titular de los datos cuando: (i) la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas, o (ii) sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

Finalmente, y en relación a este último punto, ***varios actores hablaron específicamente sobre la necesidad de regular el uso de cloud computing (o computación en la nube, como se lo denomina en español).*** Para ello, se propuso se tuvieran en cuenta los lineamientos que propone la Norma Internacional ISO/IEC 27018[31], como también guías y documentos provistos por la Cloud Security Alliance[32] y la Agencia Española de Protección de Datos[33].

IV. ACERCA DE LOS DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

En varias de las reuniones se sugirió la posibilidad de incluir algunos derechos de los titulares de los datos personales que actualmente no se encuentran contemplados en la Ley Nº 25.326.

Sobre el derecho de supresión (llamado "derecho al olvido")

Al abordar este tema, uno de los puntos sustanciales objeto de discusión fue la necesidad o no de incorporar expresamente la facultad de la DNPDP para llevar a cabo notificaciones ordenando la supresión de contenido cuando determine su incompatibilidad con la Ley Nº 25.326.

En relación a este tema, ***varios actores establecieron que la Constitución Nacional en su art. 43[34] y la Ley Nº 25.326 ya prevén una acción judicial específica para que los titulares de los datos personales puedan ejercer su derecho de supresión: la acción de hábeas data.*** Según su opinión, ésta es la única vía por la que deben transitar todos los reclamos de supresión de datos personales contra cualquiera que realice un tratamiento indebido. De esta manera, habrían interpretado que la única

autoridad competente para ordenar la remoción de contenido de la web sería la autoridad judicial.

Otros también sostuvieron que la facultad de ordenar se remuevan contenidos es exclusiva de la autoridad judicial, pero no sustentaron su posición en que la ley actual ya prevé un mecanismo para reclamar la supresión de datos personales, sino en que el derecho al olvido es un tema delicado que involucra un conflicto entre derechos de raigambre constitucional (libertad de expresión y derecho a la privacidad, el honor o la intimidad). Por este motivo, la institución más adecuada para lidiar con este tipo de controversias sería la autoridad judicial u otra de naturaleza similar, tal como lo señaló la Relatoría Especial para la Libertad de Expresión de la CIDH[35]. En este sentido, se entendería por similar un órgano con amplias facultades jurisdiccionales, que tome en consideración la naturaleza de los derechos constitucionales en juego, y respete la garantía del debido proceso, velando por la participación de todos los actores involucrados en el conflicto.

Una minoría opinó que no habría inconveniente en que la autoridad de control pudiese ordenar la remoción de contenidos, siempre y cuando la ley estipulara precisamente en qué circunstancias podría ejercerse el derecho al olvido.

En general, también se negó que el bloqueo de sitios pudiese ser una sanción válida. Máxime teniendo en cuenta que, de implementarse este tipo de sanción, sería la DNPDP quien la aplicaría, y no una autoridad judicial (a no ser que posteriormente se llevara la causa al estrado judicial). Un sector advirtió sobre los problemas que podría ocasionar tan delicada medida desde el punto de vista de la libertad de expresión. Podría presentarse la situación de que debido a la ilicitud de un contenido, se terminase bloqueando todo el sitio, con lo cual muchos otros contenidos, cuya licitud no fuese cuestionada, se verían impedidos de ser difundidos a los usuarios.

Otra discusión que se generó en torno a esta temática fue la responsabilidad de los intermediarios de Internet, a quienes comúnmente se les ordena la remoción de contenidos. En relación a esto se discutió el alcance que tiene o debería tener el derecho al olvido. De tal suerte, algunos actores destacaron que a raíz del fallo *"Rodríguez, María Belén c/ Google Inc. s/daños y perjuicios"*[36] (que no trata un caso de datos personales sino de violación de la privacidad), muchos están interpretando que se podría inferir que los motores de búsqueda de Internet quedarían sometidos a la normativa de la Ley Nº 25.326 como si efectuaran tratamiento de datos personales del contenido generado por sus usuarios.

Sin embargo, destacaron que si bien el estándar de responsabilidad subjetiva es el correcto como sanción para cualquier caso de obligaciones de remoción o bloqueo de contenidos, respecto de la Ley Nº 25.326, argumentaron que existe un debate previo a realizar. No es una cuestión de cuál estándar debería aplicar ni de cuál autoridad debe aplicarlo, sino de si se considera que los intermediarios de Internet (i) son una base de datos personales en los términos de la ley, (ii) hacen tratamiento de datos personales, y (iii) son responsable del tratamiento de datos personales.

De realizar este análisis, estos actores apuntaron que se llega a la conclusión de que la Ley Nº 25.326 no les es aplicable a los intermediarios de Internet, salvo en lo que se refiere a los datos que ellos mismos recolectan y tratan, es decir cuando actúan propiamente como responsables de los datos siendo titulares de una base de datos y decidiendo sobre los fines de su tratamiento.

La razón de esto es que los intermediarios de Internet, en particular los llamados "buscadores" indexan contenidos publicados por terceros. Sean del tipo que sea, por decisión de ese mismo tercero llamado *webmaster*. Es exclusivamente el *webmaster* quien tiene la potestad de rectificar, eliminar o editar esa información y no el intermediario. Considerar que a través de los intermediarios el titular de un dato puede ejercer en plenitud sus derechos es una falacia. Los intermediarios no tienen ningún control sobre lo que el *webmaster* hace o deja de hacer con la información que sube a Internet y que ordena, por vía de controles tecnológicos, que sea indexada por uno o algunos o todos los buscadores de Internet.

Este sector concluyó, entonces, que la Ley Nº 25.326 no se debería aplicar a los intermediarios de Internet (a excepción de cuando actúan como responsables de los datos siendo titulares de una base de datos y decidiendo sobre los fines de su tratamiento) y, por ende, no deberían ser sujetos responsables de llevar a cabo la remoción de contenidos. En todo caso, de querer exigir la supresión de un contenido se debiese responsabilizar al *webmaster* (sitio donde esa información estuviese alojada) a través de los canales que la ley vigente ya ofrece: la acción de hábeas data.

Sobre el derecho a la portabilidad de datos personales

No hubo unanimidad en relación a la implementación del derecho a la portabilidad de los datos personales, derecho contemplado por el Reglamento (UE) 2016/679[37].

Algunos destacaron que la portabilidad de los datos es técnicamente muy difícil de implementar, por lo que no debería incorporarse este derecho a la Ley Nº 25.326. Se advirtió que se debería tener sumo cuidado al querer importar todos los institutos contemplados en el Reglamento (UE) 2016/679, puesto que este Reglamento aún no ha entrado en vigencia y, por tanto, muchos institutos nuevos que en el sector académico se sospecha podrían traer aparejados problemas técnico-jurídicos (como la portabilidad de los datos) no habrían sido evaluados.

Otros, en cambio, no advirtieron este problema. Sostuvieron que las personas deberían tener la posibilidad de solicitar y obtener todos los datos que proporcionaron a la organización en formato electrónico, en un período razonable de tiempo. Opinaron que así como el Reglamento (UE) 2016/679 contempla el derecho a la portabilidad de los datos, el sistema argentino también lo debería prever siguiendo los lineamientos del Reglamento. En este sentido, un actor puntualizó que se podría ampliar la garantía contemplada en el art. 20 inc. 1 del Reglamento (UE) 2016/679 sustituyendo la restricción "que haya facilitado a un responsable del…" por "que posea un responsable del…".

Por último, un actor sugirió incorporar algunas excepciones al derecho a la portabilidad de los datos personales. Así, determinó que toda legislación relacionada con la portabilidad de datos debería dejar claro que el responsable de datos podría rechazar dicha solicitud cuando el cumplimiento de ésta implicase: (i) imponer una carga financiera o técnica excesiva sobre el responsable de datos; (ii) vulnerar la privacidad de otro usuario; (iii) vulnerar las obligaciones legales del responsable; o (iv) impedir que el responsable de datos proteja los derechos, la seguridad o los bienes del mismo, del procesador de datos, del titular o de un tercero.

V. ACERCA DE LAS OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO DE DATOS PERSONALES

Sobre el registro de bases de datos personales

Una mayoría propuso la eliminación del Registro Nacional de Bases de Datos y aquellos que no defendieron esta tesis y sostuvieron que no habría inconveniente en que se siguiese exigiendo registración de las bases de datos, recalcaron se deberían adoptar ciertas modificaciones a esta obligación.

Por un lado, el grupo mayoritario que determinó no debería existir obligación de registro de bases de datos personales sustentó su postura en distintos fundamentos: las estadísticas han demostrado que dicha obligación es una imposición de imposible cumplimiento, el registro de las bases de datos no mejora la protección de la privacidad de los titulares de los datos, la tendencia internacional en la materia es la eliminación de todo tipo de registro de bases de datos y la adopción de mecanismos proactivos o de responsabilidad demostrada (v. g. el Reglamento (UE) 2016/679 no prevé la obligación de registración).

Por otro lado, aquellos que postularon que no necesariamente se debiese eliminar el registro, puntualizaron que debería revisarse la manera en que éste se implementa en la ley vigente. Un sector estableció que debería contemplarse la situación de ciertas bases de datos privadas, pertenecientes a organizaciones o emprendimientos de tamaño reducido, para las cuales la adopción de un registro o su inscripción en el registro de base de datos puede implicar una carga difícil de soportar desde el punto de vista operativo, técnico o financiero. En este sentido, sugirieron podría disponerse la excepción de llevar registros o de inscribirse para estas organizaciones o emprendimientos de menor tamaño, en tanto las operaciones que realicen no pongan en peligro derechos fundamentales de las personas o no manejen datos sensibles. Otro sector, recalcó que un simple registro de los datos e información de contacto del sujeto responsable debería bastar, fomentando a su vez la adopción de programas de transparencia voluntaria.

Sobre las normas de responsabilidad demostrada (*Accountability*)

Hubo consenso generalizado en la necesidad de que se adopte un sistema de accountability (o normas de responsabilidad demostrada, en español). En este sentido, se recomendó se tengan como referencia el APEC Cross Border Privacy Rules system[38] y el modelo mexicano de protección de datos personales[39].

A su vez, un actor refirió a la certificación de ciertos estándares internacionales, así como la ISO/IEC 27018, como una manera que cuentan las empresas de demostrar estar tomando los recaudos necesarios para la protección de los datos personales que tratan. Según su opinión, el reconocimiento internacional de estos programas podrá proveer uniformidad y consistencia a la materia, facilitando la tarea de los órganos de control y evaluación por parte de los usuarios de servicios (titulares de los datos) y sin correr el riesgo de tornarse en un sistema sumamente burocrático. Se destacó que las normas ISO han sido y están siendo reconocidas mundialmente por distintos agentes reguladores/órganos de control como un mecanismo de acreditar buenas prácticas y el cumplimiento de normativas.

En relación a las eventuales inspecciones, un actor destacó que es necesario se disponga expresamente (en la ley o en su correspondiente reglamentación) que la DNPDP tendrá la facultad de exigir al responsable de tratamiento exhibir la documentación pertinente que acredite la implementación de medidas apropiadas, pero no podrá, en cambio, exigir se acompañe la documentación, es decir, exigir se le deje una copia de la documentación. De esta manera, se evitará ocurran eventuales filtraciones de información y que, ante el temor de éstas, los responsables de tratamiento de datos terminen demostrando menos de lo que efectivamente hacen para asegurar la privacidad de los datos personales que tratan.

Sobre un modelo basado en el riesgo

Varios actores propusieron se incluya en la Ley Nº 25.326 el concepto de "enfoque basado en el riesgo", convirtiendo en responsabilidad de las organizaciones la evaluación del riesgo y el impacto del procesamiento de la información de los individuos y las acciones para mitigarlo. Esto les permitiría priorizar, ser más eficientes y enfocarse en el riesgo potencial. Solo en caso de que el proceso resultante fuese considerado como de alto riesgo debería ser restringido o prohibido con carácter ex-ante.

Se sugirieron varios ejemplos a tomar de referencia que adoptan un enfoque basado en el riesgo.

En primer lugar, se hizo mención del Reglamento (UE) 2016/679, que incentiva a los responsables de tratamiento de datos a implementar medidas proactivas correspondientes al nivel de riesgo de sus actividades. Así, el Reglamento obliga a las organizaciones a implementar un nivel de seguridad adecuado al riesgo, a hacer una evaluación de impacto relativa a la protección de datos, a notificar a la autoridad de control ante una violación de seguridad de los datos, entre otras medidas.[40]

En segundo lugar, se recomendó se tomara de referencia el *European Privacy Impact Assesment Handbook* publicado por la Oficina del Comisionado de Información del Reino Unido (ICO) en 2007[41], así como la Guía para una Evaluación de Impacto en la Protección de Datos Personales, publicada por la Agencia Española de Protección de Datos Personales en 2014[42].

Además se destacó que desde la entrada en vigor del E-Government Act de 2002[43], todas las agencias federales de EEUU deben cumplir con Evaluaciones de Impacto de Privacidad. Lo mismo ocurre con las agencias gubernamentales de Reino Unido desde 2008[44].

Por último, se señaló que las leyes que exigen se realice una notificación ante incidentes de seguridad en Europa, Australia, Canadá, México, Nueva Zelanda y Estados Unidos, entre otros, estarían actualmente requiriendo se efectúe una evaluación del riesgo implicado en la pérdida o exposición de información.

Sobre el diseño desde la privacidad y por defecto (*Privacy by design – Privacy by default*)

Algunos actores abordaron este tema, sugiriendo se implementen los principios de *privacy by design* y *privacy by default* en la Ley Nº 25.326.

Se opinó que el principio de *privacy by design,* entendido como un enfoque en el que el impacto en la privacidad de cualquier nuevo sistema, proceso o servicio debe ser contemplado desde las fases iniciales del ciclo de vida de su desarrollo, no debiese ser el único mecanismo de *enforcement* en el diseño de nuevos sistemas o servicios a brindar debido a que su implementación es voluntaria. De esta manera, se defendió que la Ley Nº 25.326 debiese contemplar también el principio de *privacy by default*, que exige se fije la configuración de privacidad de los usuarios de un nuevo sistema, por defecto, en términos tales que provean el máximo nivel de protección. Estos dos principios han sido previstos en el Reglamento (UE) 2016/679[45], por lo que podrían seguirse sus lineamientos.

Un sector estableció, en cambio, que estos principios podrían formar parte de recomendaciones de la DNPDP sobre privacidad, pero no sería conveniente se incorporaran a la ley, puesto que implicarían una posible amenaza para la industria del marketing o la publicidad (v. g. la adecuación a los requerimientos de estos nuevos institutos implicaría costos económicos elevados).

Sobre la figura del Delegado de Protección de Datos Personales

Muchos de los actores que intervinieron en el proceso de consulta apoyaron la inclusión de la figura del Delegado de Protección de Datos (en adelante "DPO"), que ha sido contemplada en el Reglamento UE 2016/679[46]. Sin embargo, la mayoría planteó interrogantes a ser evaluados a la hora de adoptar su implementación.

En general, se recalcó la necesidad de evaluar cómo se resolverá la implementación del DPO en una PyME. En este sentido, habría que evaluar si todas las PYME que manejasen bases de datos personales deberían tener un DPO, como también analizar si podría darse la posibilidad a las PyME de que capacitaran a una persona para que cumpliera la función de DPO además de cumplir otras funciones en la empresa, y así reducir eventuales costos. En relación a este punto, se sugirió se analizara si verdaderamente es necesario exigir que el DPO tuviese título de abogado o, si en cambio, pudiese ser profesional de otra carrera vinculada a la materia de protección de datos (v. g. Ingeniería, Sistemas). A su vez, podría contemplarse la posibilidad de que ciertas empresas pudiesen "tercerizar" la actividad del DPO.

Varios participantes de las reuniones opinaron que es inviable que absolutamente todos los organismos estatales cuenten con un DPO. Por tal motivo, se advirtió será necesario definir el criterio a seguirse para la adopción del DPO en el sector público, esto es, cuáles organismos deberán tener obligatoriamente un DPO y cuáles no.

No hubo consenso en relación a las atribuciones que debería tener el DPO. Algunos opinaron que el DPO no sólo debería ser un interlocutor con la DNPDP sino también con los particulares. Mientras que otros sostuvieron que, de implementarse la figura del DPO, éste debería actuar exclusivamente como punto de contacto con la autoridad de control. Este último sector defendió que la manera en que las organizaciones atienden los reclamos de los particulares en torno a sus derechos debería quedar librada a la autorregulación de cada organización. Según se destacó, hoy día exigirle a las empresas contar con un DPO para atender los reclamos o consultas de los particulares es una ficción porque lo termina resolviendo un equipo o sector de la empresa.

Asimismo, un participante opinó se debería considerar de manera flexible la situación de muchas organizaciones multinacionales que operan en Argentina que tienen un DPO y una Oficina Central de Privacidad que no están ubicadas en Argentina pero que, sin embargo, son responsables por la recolección y procesamiento de datos de los empleados de las sucursales argentinas y de sus clientes. A lo mejor, en estos casos no tendría sentido requerir se designara un DPO local (en Argentina) puesto que su función ya estaría siendo cumplida en el exterior.

En relación a todas estas discusiones, un actor advirtió sobre la importancia de aguardar a que el Grupo Europeo de Protección de Datos del Artículo 29 (en adelante "Grupo de Trabajo del Artículo 29" o "GT 29")[47] desarrolle aclaraciones sobre la implementación de la figura del DPO contemplada en el Reglamento UE 2016/679 y efectuó algunas sugerencias al respecto, que podrían tenerse en cuenta de adoptar en Argentina similares disposiciones.

En primer lugar, se hizo referencia al art. 37 inc. 1 del Reglamento UE 2016/679 que indica en qué circunstancias se debe designar obligatoriamente un DPO. El apartado (b) de este artículo establece que se deberá designar un DPO siempre que "las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala". Los términos "habituales", "sistemáticos" y "gran escala" son vagos y requieren de mayor precisión. Conforme la opinión de este actor, se debiese permitir a las organizaciones decidir libremente si su actividad encuadra o no en esta descripción, y eventualmente que la autoridad de control pueda exigir a las organizaciones demostrar el criterio aplicado para decidir sobre la designación del DPO.

En segundo lugar, se destacó se debería clarificar que mientras haya un DPO como responsable "principal", no habría inconveniente de que las tareas del DPO fueran llevadas a cabo por un equipo (interno dentro de la misma organización o incluso contratando asesores externos). A su vez, se estableció que, dada la multiplicidad de conocimientos y aptitudes que debería tener el DPO, las variadas responsabilidades y su rol estratégico en las organizaciones, sería conveniente que el DPO tuviera una posición *senior* dentro de la organización. Adicionalmente, se indicó que la ubicación geográfica del DPO no debería afectar al debido cumplimiento de sus tareas, siempre y cuando el DPO cumpliese efectivamente con sus responsabilidades.

En tercer lugar, se puntualizó que el deber del DPO de "mantener el secreto o la confidencialidad" que exige el art. 38 inc. 5 del Reglamento UE 2016/679 podría eventualmente ocasionarle un conflicto al DPO, quien se supone debe cumplir sus funciones dentro de una organización, cooperando con aquella e incluso siendo transparente. Por este motivo, se sugirió que, de implementar esta misma provisión en la Ley Nº 25.326, se interprete ampliamente de modo que permita llegar a una solución viable y razonable en relación a los tipos de información que deben mantenerse confidenciales.

De igual modo, se sugirió que, en caso de incluir el concepto de "conflicto de intereses" provisto por el art. 38 inc. 6 del Reglamento UE 2016/679 dentro de la ley, se adopte una interpretación amplia de éste. Conforme el art. 38 inc. 6, el DPO "podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses." La experiencia ha demostrado que los DPO pueden combinar

satisfactoriamente sus funciones con otros roles, como Oficial de Gobernanza de la Información (*Information Governance Officer*) y Jefe de Estrategia de Información (*Chief Data Strategist*). Es de la esencia misma del DPO tener un amplio espectro de habilidades y aptitudes para cumplir mejor sus funciones dentro de la organización. De interpretar restrictivamente el art. 38 inc. 6 del Reglamento se podría correr el riesgo de restringir el correcto desempeño del DPO.

Por último, respecto a la función del DPO de "cooperar con la autoridad de control" y de "actuar como punto de contacto de la autoridad de control", que se extrae del art. 39 inc. 1 (d) y (e) del Reglamento, se estipuló que es importante no interpretar esto como una obligación por parte del DPO de actuar como denunciante frente a la autoridad de control. ***El DPO debe permanecer como un asesor de confianza dentro de la organización y un punto de contacto organizacional con la autoridad de control que responderá ante sus consultas. Es fundamental se tenga en cuenta este punto para una futura reforma de la Ley Nº 25.326.***

VI. ACERCA DE ALGUNOS SUPUESTOS ESPECIALES DE TRATAMIENTO

Sobre el tratamiento de datos por organismos públicos

Varios actores coincidieron en que la Ley Nº 25.326 le otorga al Estado demasiadas prerrogativas en lo que hace al manejo de datos personales de los particulares. Actualmente muchas de las garantías establecidas en la ley no son aplicables a las bases de datos estatales. De esta manera, el Estado cuenta con una excesiva permisibilidad para almacenar, tratar y ceder datos personales. Por ello, se considera que la discusión sobre una reforma de la ley debería incluir una limitación de las capacidades que el Estado tiene para realizar operaciones con datos personales.

Se sugirieron, como posibles limitaciones, la adopción del requisito de consentimiento para algunos casos, o el requisito de interés legítimo para aquellos casos en que no fuese factible requerir el consentimiento, en virtud de las necesidades propias de los órganos estatales. Asimismo, se propuso analizar la conveniencia de la incorporación explícita de que el Estado también deba cumplir con los demás principios que conforman el sistema, en particular el principio de finalidad y el principio de adecuación y pertinencia de los datos. Por último, y en relación a este último punto, se sugirió que la Ley Nº 25.326 contemplase mecanismos que desmotivaran al funcionario del uso de ciertas bases de datos personales para finalidades que estuvieran por fuera de su competencia.

Sobre el tratamiento de datos por organismos de seguridad e inteligencia

Un actor indicó sería necesario revisar el marco normativo que regula las bases de datos que poseen las fuerzas armadas, las fuerzas policiales, y otras fuerzas de seguridad. Según su opinión, la futura legislación debería establecer mayores obligaciones que restrinjan la discrecionalidad con que las fuerzas armadas y de seguridad manejan sus bases de datos.

Entre las limitaciones que podrían incluirse se mencionaron: (i) la necesidad de establecer plazos para la supresión de los datos personales o para su revisión periódica, a fin de evaluar la pertinencia de su almacenamiento; (ii) establecer la distinción entre datos personales recabados en base a hechos, de aquellos que puedan derivarse de apreciaciones personales, opiniones, juicios de valor propios de los agentes que realizan las tareas de seguridad o de defensa; (iii) consagrar los derechos de acceso, rectificación y supresión, con las limitaciones que surjan de la necesidad de llevar adelante una investigación eficaz. A su vez, se destacó que (iv) si bien puede resultar razonable no exigir el consentimiento del titular para la eficacia de la investigación, se debería establecer claramente que el resto de los principios de la legislación de protección de datos debe ser respetado. Por último, y como otra limitación, se estableció que (v) en caso de que se utilizaran tecnologías para el tratamiento de datos que tuvieran el riesgo de resultar fuertemente invasivas de la privacidad, debería realizarse ex ante una evaluación de impacto sobre datos personales, con participación de la autoridad de contralor.

Sobre el tratamiento para servicios de información crediticia

Aquellos actores que hicieron referencia a los servicios de información crediticia, coincidieron en que ciertas disposiciones de la ley vigente en relación a este tema debieran revisarse. Entre las propuestas a ser evaluadas en una eventual reforma de la Ley Nº 25.326 se mencionaron: (i) la necesidad de que la Ley Nº 25.326 defina precisamente el momento a partir del cual debe computarse el plazo de conservación de información de una deuda en mora; (ii) contemplar la obligación de informar cuando se utilice un informe de riesgo crediticio para denegar la celebración de un contrato; (iii) prever que ante una cesión de carteras de créditos por parte de entidades financieras, actividad que es parte del giro ordinario de los negocios de los bancos, no sea necesario obtener el consentimiento expreso del titular de los datos objeto de cesión (sin perjuicio de requerir notificación).

Hubo disparidad de opiniones cuando se discutió sobre la posibilidad de prever la obligación por parte del acreedor de notificar al deudor antes de ceder información de incumplimientos patrimoniales a los bancos de datos que prestan servicios de información crediticia. Un sector estuvo de acuerdo en contemplar esta obligación en la ley. Mientras que otro sector destacó que la implementación de esa obligación probablemente resultara en la práctica muy engorrosa.

Por último, un sector propuso sería conveniente se permitiera, al igual que en otros países, que entre organismos estatales de distintas jurisdicciones y algunas instituciones privadas (v. g. entidades financieras), se permitiera el libre flujo de información que identificara a personas sospechosas de haber cometido actos de lavado de dinero o actos de terrorismo.

Sobre el tratamiento de datos contenidos en bases de datos con fines de publicidad

Sólo algunos actores hicieron referencia al tratamiento que se le da en la ley vigente al uso de las bases de datos con fines de publicidad.

Un actor sugirió que la Ley Nº 26.951 referida al Registro No Llame podría receptarse dentro del art. 27 de la Ley Nº 25.326, modificando algunas de sus disposiciones y corrigiendo errores (v. g. el art. 8 de la Ley Nº 26.951, al establecer las excepciones a la ley, refiere a campañas de bien público "tal como lo dispone la Ley Nº 25.326" y la Ley Nº 25.326 no hace ninguna referencia a campañas de bien público).

Otro actor sugirió que el art. 27 de la Ley Nº 25.326, referido a las bases de datos con fines de publicidad, figure de forma destacada dentro de un capítulo de Regímenes Especiales. A su vez, advirtió sobre la existencia de un error sintáctico en su inc. 1, sugiriendo se reemplace un punto y coma por una coma, dado que como está redactado actualmente presta a confusión.

Por último, un actor criticó la manera en que la ley regula las bases de datos con fines de publicidad, puesto que bajo su criterio, otorga demasiadas libertades a las empresas que hacen uso de los datos personales para fines publicitarios, dejando de lado criterios y principios generales establecidos en la ley.

Sobre el tratamiento de grandes volúmenes de datos (*Big Data*)[48]

Durante la serie de reuniones se hizo referencia a *Big Data*, sus implicancias en la actualidad y las discusiones y desafíos que plantea. Sin embargo, en general, no se recalcó la necesidad de incluir este concepto a la Ley Nº 25.326.

Al abordar este tema, un participante de las reuniones sugirió algunos modelos a tomarse en cuenta para evaluar cómo tratar el manejo y análisis de *Big Data*. De tal suerte, señaló se podría tomar de referencia el *Unified Ethical Frame for Big Data Analysis,* modelo que está siendo desarrollado por la fundación Information Accountability Foundation,[49] que aborda temas relacionados a *Big Data* y se encuentra respaldado por reguladores y empresas, entre otros. A su vez, también se recomendó se tuviese en cuenta el modelo publicado por la Oficina Ejecutiva del Presidente de EEUU, denominado *Big Data: Seizing Opportunities, Preserving Values*[50].

VII. ACERCA DE LA AUTORIDAD DE APLICACIÓN Y CONTROL DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

Sobre el diseño institucional

Todos los actores que hicieron referencia al órgano de control y su diseño institucional coincidieron en que sería necesario que la Ley Nº 25.326, de reformarse, contemplara una expansión de la capacidad de la DNPDP para cumplir con sus deberes de contralor. Para lograr este objetivo, se destacó que resultaría necesario aumentar la autonomía de la DNPDP y garantizar su adecuado financiamiento. Incluso, se sugirió se analizara la posibilidad de tener un órgano de control con capacidad presupuestaria propia.

Se propusieron algunos mecanismos para reforzar la posición de la autoridad de control y dotarla de mayor autonomía. Por un lado, se indicó que sería conveniente analizar, como punto de partida, la reincorporación al cuerpo normativo de los dos

apartados de la ley que fueran observados bajo el Decreto Nº 995/2000.[51] Por otro lado, se estableció que para la remoción del Director Nacional de Protección de Datos Personales se deberían adoptar similares mecanismos a los previstos para su designación. Por último, se sugirió se previera la posibilidad de que las disposiciones de la DNPDP fuesen vinculantes.

Asimismo, se advirtió sobre el riesgo que se corre al delegar al Poder Judicial toda discusión sobre la protección de los datos personales. Algunos actores expresaron que los jueces, por lo general, tienen poco conocimiento sobre el tema, por lo que sus decisiones no suelen responder a la inmediatez que requiere el proceso de hábeas data. Por este motivo, se resaltó la importancia de reforzar la posición de la autoridad de control, órgano especializado en la materia, para que sea en todos los casos quien primero tenga contacto con las problemáticas que surgen en relación a los datos personales, logrando que el control judicial sea *ex post* (en caso de ser necesario).

Vinculado con la reciente aprobación de la Ley de Acceso a la Información Pública (Ley Nº 27.275) se planteó la discusión respecto a si no debiese ser la misma autoridad la que aplicase las dos normativas, en lugar de tener dos entidades administrativas diferentes, así como sucede en otros países[52]. Asimismo, aquellos que hicieron referencia a este tema, recalcaron la importancia de compatibilizar la eventual reforma de la Ley Nº 25.326 con la nueva Ley de Acceso a la Información Pública.

Sobre las sanciones que aplica la autoridad de aplicación

Muchos actores reconocieron sería necesaria una revisión y actualización de las sanciones vigentes. Se advirtió, sin embargo, que de establecer un mecanismo de actualización automática del monto de las multas, fijar las ganancias del infractor como un valor de referencia sería problemático para muchas industrias e incluso injusto. Como regla, las sanciones deben ser proporcionales al daño y no a las ganancias del infractor.

Por otro lado, un sector estableció que la cancelación de las bases de datos o el bloqueo de sitios web no sería ser una sanción administrativa válida. Algunos indicaron que prever estas sanciones administrativas atentaría contra el derecho de ejercer toda industria lícita, y en el caso de bloqueo de sitios, también contra la libertad de expresión y el principio de neutralidad en la red. En este sentido, señalaron que por ejemplo, en el eCommerce, el sitio web es el negocio, por lo que bloquear el sitio significaría cerrar el negocio. Lo mismo ocurriría en caso de cancelar la base de datos a empresas que desarrollan sus ventas por marketing directo (postal, telefónico, email, etc.), en las que sin base de datos no podrían realizar sus negocios. Otros meramente opinaron que el bloqueo de sitios web o la cancelación de las bases de datos no serían una sanción administrativa válida en la medida en que no se previesen claras directrices que indicaran hasta qué límite y bajo qué circunstancias se podría ordenar dicha sanción.

PARTICIPANTES

Académicos y particulares

- Alejandro Castillo
- Juan Darío Veltani
- Guillermo F. Peyrano
- Horacio R. Granero
- Leonor Guini
- Mariano Javier Peruzzotti
- Mariano M. Del Río
- Matilde S. Martínez
- Natalia Eugenia Roda
- Oscar Puccinelli
- Pablo A. Palazzi
- Paula Vargas
- Silvia Iglesias

Sector privado

- Accenture
- Asociación de Bancos Argentinos (ADEBA)
- Asociación de Bancos de la Argentina (ABA)
- Asociación de Marketing Directo e Interactivo de Argentina (AMDIA)
- Cámara Argentina de Comercio Electrónico (CACE)
- Cámara Argentina de Internet (CABASE)
- Cámara de Comercio de los Estados Unidos de América en la Argentina (AmCham Argentina)
- Confederación Argentina de la Mediana Empresa (CAME)
- Facebook
- Google
- GSMA
- IBM
- Information Technology Industry Council(ITI)
- INTEL
- MercadoLibre
- Microsoft
- Telecom
- Telefónica

Sociedad civil

- Asociación Civil por la Igualdad y la Justicia (ACIJ)
- Asociación por los Derechos Civiles (ADC)
- Centre for Information Policy Leadership (CIPL)
- Fundación Poder Ciudadano
- Fundación Sadosky
- Fundación Vía Libre
- Information Accountability Foundation (IAF)

[1] Para mayor información sobre la plataforma "Justicia 2020", acceda al sitio: https://www.justicia2020.gob.ar/ última consulta: 06/12/2016
[2] Para mayor información, acceda al comunicado de prensa de la DNPDP en el sitio: http://www.jus.gob.ar/datos-personales/comunicados/2016/05/31/politicas-de-privacidad-direccion-de-proteccion-de-datos-personales-impulsa-modificacion-de-la-ley-25326.aspx última consulta: 06/12/2016
[3] Publicación oficial: http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx última consulta: 05/12/2016
[4] Publicación oficial: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf última consulta: 05/12/2016. Ver puntualmente los arts. 47 y 48 del Reglamento (UE) 2016/679.
[5] Publicación oficial: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm última consulta: 05/12/2016
[6] Comisión de las Comunidades Europeas - Decisión de la Comisión C (2003)1731 de 30/06/2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina. Publicación oficial: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf última consulta: 05/12/2016
[7] Publicación oficial: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES última consulta: 05/12/2016
[8] Publicación oficial: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx última consulta: 05/12/2016
[9] Publicación oficial: http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx última consulta: 05/12/2016
[10] Publicación oficial: https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text última consulta: 05/12/2016
[11] Publicación oficial: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf última consulta: 05/12/2016
[12] Publicación oficial: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/texact.htm última consulta:05/12/2016
[13] Código Civil y Comercial de la Nación, Libro Sexto: Disposiciones comunes a los derechos personales y reales, Título I, Prescripción y caducidad.
[14] Publicación oficial: http://www.corteidh.or.cr/docs/opiniones/seriea_22_esp.pdf última consulta: 05/12/2016
[15] El artículo 36 de la Ley Nº 25.326 establece:
"Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.
Procederá la competencia federal:
a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y
b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales."
El artículo 44 de la Ley Nº 25.326 establece:
"Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.
Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.
La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional."
[16] Ver fallo "Rodríguez, Carina Roxana c. Banco Hipotecario S.A. s/ Hábeas data", CSJN, 25/11/08, R.1021.XLIII. Asimismo en "Svatzky, Betina Laura c/ Datos Virtuales S.A. s/ Hábeas data", CSJN, 03/05/2005, Fallos: 328: 1252, la Corte afirmó la competencia federa respecto de bases de datos situales en Internet.
[17] Publicación oficial: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf última consulta: 05/12/2016
[18] Publicación oficial: http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?CompId:2f46a4ee-0962-49e4-8e8d-eac45eff42b2 última consulta: 05/12/2016
[19] Publicación oficial: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf última consulta: 05/12/2016. Ver puntualmente los arts. 8, 9 y 10 de la ley, que refieren al principio del consentimiento.
[20] Publicación oficial: http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf última consulta: 05/12/2016. Ver específicamente la siguiente sección: Schedule 1 - Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information CAN/CSA-Q830-96, 4.3 Principle 3 – Consent.
[21] El artículo 6 inc. 1 (b) del Reglamento (UE) 2016/679 establece:
"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:... (b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales..."
[22] El artículo 6 inc. 1 (f) del Reglamento (UE) 2016/679 establece:
"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:... (f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."

[23] El artículo 8 del Reglamento (UE) 2016/679 establece:
"Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información
1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.
2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.
3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño."
[24] El artículo 7 de la Ley Estatutaria 1581 establece:
"Derecho de los niños, niñas y adolescentes. En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.
Queda proscrito el Tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública.
Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás. El Gobierno Nacional reglamentará la materia, dentro de los seis (6) meses siguientes a la promulgación de esta ley."
[25] El artículo 33 del Reglamento (UE) 2016/679 establece:
"Notificación de una violación de la seguridad de los datos personales a la autoridad de control
1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:
a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.
5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."
[26] Por ejemplo, en el estado de Washington se prevé que en caso de que se deba notificar a más de 500 residentes de ese estado ante un incidente de seguridad, quien esté obligado a efectuar la notificación a los afectados deberá notificar también al Fiscal General (RCW 19.255.010. Publicación oficial: http://app.leg.wa.gov/RCW/default.aspx?cite=19.255.010 última consulta: 05/12/2016) Lo mismo ocurre en el estado de California (California Civil Code, Section 1798.82. Publicación oficial: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82 última consulta 05/12/2016) Así también en el estado de Florida, donde en caso de que la notificación por incidentes de seguridad se efectúe a 500 residentes o más, se debe notificar al Departamento de Asuntos Legales de Florida (Florida Statutes, Section 501.171. Publicación oficial: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html última consulta: 05/12/2016)
[27] Por ejemplo, en Florida se da un plazo adicional de 15 días para efectuar la notificación ante el Departamento de Asuntos Legales de Florida siempre y cuando haya motivos justificados (Florida Statutes, Section 501.171. Publicación oficial: http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html última consulta: 05/12/2016)
[28] Publicación oficial: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional última consulta: 05/12/2016

[29] Por ejemplo, el Reglamento (UE) 2016/679 autoriza que se realicen transferencias internacionales de datos personales a un tercer país u organización internacional si el responsable o el encargado del tratamiento hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. (Ver art. 46 del Reglamento (UE) 2016/679)

[30] El artículo 37 de la Ley Federal de Protección de Datos en Posesión de los Particulares establece:

"Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

VII. *Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular."*

[31] Publicación oficial: http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498 última consulta: 05/12/2016

[32] Por ejemplo, ver: https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf última consulta: 06/12/2016

[33] Por ejemplo, ver: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf última consulta: 06/12/2016

[34] El artículo 43 de la Constitución Nacional establece:

"Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.

Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización.

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de hábeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio." (El énfasis nos pertenece)

[35] Ver, por ejemplo, la Declaración Conjunta realizada por el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión de Derechos Humanos de la OEA en 2012. Publicación oficial: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=888&lID=2 última consulta: 06/12/2016

[36] Publicación oficial: http://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumento.html?idAnalisis=716258&interno=1 última consulta: 05/12/2016

[37] El artículo 20 inc. 1 del Reglamento (UE) 2016/679 establece:

"Derecho a la portabilidad de los datos

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. *El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros."*

[38] Publicación oficial: http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx última consulta: 05/12/2016

[39] Publicación oficial: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf última consulta: 05/12/2016. Ver puntualmente los arts. 47 y 48 del Reglamento (UE) 2016/679.

[40] Publicación oficial: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679 última consulta: 05/12/2016. Ver puntualmente los arts. 32 a 36 del Reglamento (UE) 2016/679.

[41] El Reino Unido fue el primer país de Europa en desarrollar y promulgar una metodología de Evaluación de Impacto de la Privacidad. La Oficina del Comisionado de Información (ICO) publicó un Manual en diciembre de 2007, seguido de una revisión en junio de 2009. En 2013, Trilateral Research & Consulting publicó un informe destinado a que se efectúe una revisión de las Guías de Evaluación de Impacto de Privacidad. En 2014 la ICO publicó el Código de Práctica sobre la realización de Evaluaciones de Impacto sobre la Privacidad que reemplazó al Manual de Evaluación de Impacto de la Privacidad. Publicación oficial: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf última consulta: 06/12/2016

[42] Publicación oficial: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf última consulta: 05/12/2016

[43] Publicación oficial: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf última consulta: 05/12/2016

[44]La Oficina del Gabinete del Reino Unido estableció que, a partir de 2008, todos los organismos y agencias gubernamentales estarían obligados a cumplir con Evaluaciones de Impacto de Privacidad (*PIA reports*). Para mayor información acceder a: https://ico.org.uk/media/for-organisations/documents/1042837/trilateral-report-executive-summary.pdf última consulta: 06/12/2016

[45] El artículo 25 del Reglamento (UE) 2016/679 establece:

"Protección de datos desde el diseño y por defecto

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los *datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.*

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."

[46] Publicación oficial: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679 última consulta: 05/12/2016. Ver puntualmente los arts. 37 a 39 del Reglamento (UE) 2016/679.

[47] El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Las autoridades de los estados candidatos a ser miembros de la Unión y los países del EEE asisten a sus reuniones como observadores.

El GT 29 cuenta con un presidente y dos vicepresidentes, elegidos de entre sus miembros por periodos de dos años, renovables. Se reúne en plenarios con una periodicidad bimestral y organiza sus trabajos a través de diversos subgrupos temáticos, que preparan las decisiones del plenario.

Las funciones del GT29 reconocidas por la Directiva incluyen estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea.

El GT 29 se pronuncia a través de Dictámenes, Documentos de Trabajo, Informes o Recomendaciones, aunque también manifiesta su posición en cartas o comunicados de prensa. Las decisiones del Grupo no son jurídicamente vinculantes, pero tienen un importante valor doctrinal y son frecuentemente utilizados y citados por los legisladores y los tribunales nacionales y europeos.

[48] Conforme la opinión de uno de los participantes de las reuniones, se denomina *Big Data* al fenómeno mediante el cual vastos conjuntos de datos procedentes de diversas fuentes se combinan y se analizan a través de potentes ordenadores para extraer conclusiones acerca de, e influir en el comportamiento - especialmente el comportamiento humano.

[49] Publicación oficial: http://informationaccountability.org/wp-content/uploads/IAF-Unified-Ethical-Frame.pdf última consulta: 05/12/2016

[50] Publicación oficial: https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf última consulta: 05/12/2016

[51] Los apartados 2 y 3 del artículo 29 de la Ley Nº 25.326 fueron observados. Estos apartados establecen lo siguiente:
2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.
3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

[52] Por ejemplo, México cuenta con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que es el organismo competente de garantizar en el Estado mexicano los derechos de las personas a la información pública y a la protección de sus datos personales. El INAI es un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio.