EL SISTEMA DE PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

Oportunidades y desafíos para los derechos humanos

VOLUMEN I

por los Derechos Civiles

Área de Privacidad

Diciembre 2016
https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por la Ford Foundation, el mismo es publicado bajo una licencia Creative Commons Atribución - No Comercial - Compartir Igual. Para ver una copia de esta licencia, visite https://creativecommons.org/licenses/by-nc-sa/2.5/.

El documento *El sistema de protección de datos personales en América Latina: Oportunidades y desafíos para los derechos humanos* es de difusión pública y no tiene fines comerciales.

Índice

El sistema de protección de datos personales en América Latina:

Oportunidades y desafíos para los derechos humanos*

I Resúmen ejecutivo

En el presente documento la Asociación por los Derechos Civiles propone el análisis comparativo de los sistemas de protección de datos personales vigentes en Argentina, Brasil, Chile y México, tanto entre sí como a la luz de las disposiciones del Reglamento General de Protección de Datos (RGPD) de la Unión Europea. La finalidad última del documento es identificar oportunidades y desafíos para los derechos humanos a la luz del rol que los datos personales han adquirido en virtud del desarrollo tecnológico.

Para la realización de este trabajo, se tomó como base las investigaciones llevadas a cabo por la Asociación por los Derechos Civiles (ADC) en Argentina, Internet Lab en Brasil, Derechos Digitales en Chile y Red por la Defensa de los Derechos Digitales (R3D) en México, mencionadas en el punto 5.5.2.

El trabajo comienza con una explicación del surgimiento de la legislación sobre protección de datos personales y su posterior expansión, producto del desarrollo tecnológico y la aparición de prácticas comerciales que colocaron al manejo de datos personales en el centro del modelo de negocios de numerosas compañías. Luego, se da cuenta del nacimiento de estándares internacionales que buscan regular y neutralizar las potenciales lesiones que el tratamiento de los datos personales puede provocar en los derechos de las personas.

A continuación, se menciona el desarrollo que la protección de datos personales tuvo en Europa, desde su aparición como un derecho autónomo –distinto de otros derechos como la privacidad o la

*El presente informe fue redactado por **Valeria Milanes**, Directora de las áreas de Privacidad y Libertad de Expresión de la Asociación por los Derechos Civiles (ADC). Encargado de diseño: **Leandro Ucciferri**, abogado e investigador de las áreas de Privacidad y Libertad de Expresión de la ADC.

intimidad- hasta la adopción del flamante Reglamento General para la Protección de Datos de la Unión Europa. Después de este repaso, tiene lugar el núcleo central del trabajo: una comparación entre las disposiciones normativas de los países latinoamericanos analizados, a los fines de detectar las similitudes y diferencias al momento de regular la protección de datos personales. Además de la comparación entre países, la normativa también es evaluada con respecto al Reglamento General debido a los altos estándares protectorios que establece y a su recepción normativa del fenómeno de las nuevas tecnologías.

Finalmente, se ofrecen conclusiones y recomendaciones, cuyo objetivo es establecer un punto de partida para el debate entre todos los sectores interesados en la temática acerca de las mejores formas de incrementar la defensa de los derechos de las personas frente a posibles abusos en el tratamiento de sus datos.

II Contexto: El rol de los datos personales

i Nociones generales

Las primeras normativas vinculadas a la protección de datos personales tuvieron su origen en la década de 1960 y 1970, cuando el desarrollo tecnológico era incipiente.

Así, según el análisis que la Organización para la Cooperación y Desarrollo Económico (OCDE) realizó en ocasión de la actualización de las Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales en el año 2013[1], más de 30 años después, los avances en el entorno tecnológico y digital han sido abrumadores. El volumen y los múltiples usos de los datos personales, se han disparado debido a lo sencillo que resulta la recolección, el almacenamiento, el procesamiento, la agregación, el análisis y la transferencia de enormes cantidades de datos.

Los avances en el poder de la computación combinados con el fácil acceso a dispositivos fijos y móviles conectados globalmente a través de internet han transformado el rol de los datos personales en la economía y en la sociedad. El cambio de tecnología analógica a tecnología digital en las comunicaciones y en el entretenimiento ha provocado una mayor capacidad para almacenar y compartir datos personales, y más notablemente fotografías, audios, filmaciones e imágenes en video.

Los datos personales son, cada vez más, el activo central para las operaciones de negocios y también resultan esenciales para una administración de gobierno efectiva.

[1] "Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales" de la Organización para la Cooperación y el Desarrollo Económico - OCDE (2013), pág. 81 y ss. Accesible en https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm en inglés. Visitado en enero 2017.

ii El desarrollo tecnológico

Los diversos desarrollos tecnológicos profundizan esta marcada tendencia de recolección y uso de los datos personales.

Las redes de comunicación, mediante de computadoras interconectadas a través de internet, y la variadas posibilidades de conexión a través de trasmisiones por satélite, por cable y por fibra óptica han aumentado el acceso y la capacidad de transferencia de los datos. Los nuevos dispositivos, una mayor interoperabilidad y un enorme crecimiento de las tecnologías inalámbricas también han contribuido al incremento en la tasa de transferencia de los datos.

El incremento en la cantidad de computadores personales en hogares y lugares de trabajo ha sido vertiginoso, y más recientemente, han surgido los dispositivos móviles, incluyendo a los teléfonos inteligentes (*smartphones*). Estos dispositivos en particular, poderosos y portátiles, combinan datos de geolocalización y conexión a internet, lo que permite el desarrollo de un amplio campo de nuevos servicios y aplicaciones, muchos de los cuales dependen de de la recolección y uso de la información personal para generar ganancias. Además del acceso a internet, muchos de estos dispositivos contienen herramientas que permiten la captura de imágenes, sonido y datos de localización. El potencial de estos dispositivos para capturar y distribuir imágenes y para hacer el seguimiento de la localización y los movimientos de los individuos, muchas veces sin que éstos lo sepan, ha crecido significativamente.

Por otro lado, los costos de almacenamiento de información digitalizada han bajado significativamente, por lo que se puede guardar por largos períodos o en forma indefinida. El volumen de la información de los datos personales mantenidos por organizaciones e individuos también se ha expandido. Las prácticas de almacenamiento están evolucionando, ya que las organizaciones y los individuos están utilizando servicios de almacenamiento provisto por terceros, cuyas bases de datos pueden estar localizadas en otro país.

Las herramientas para el procesamiento de datos son cada vez más poderosas, sofisticadas, ubicuas y baratas, lo que permite que la información sea fácil de buscar, de vincular y de ubicar para diversos actores, no sólo los gobiernos o las grandes corporaciones.

El desarrollo y el uso de algoritmos y herramientas analíticas han permitido el acceso a enormes conjuntos de datos y han posibilitado que estos datos puedan conectarse, lo que resulta en más y nuevos usos de los datos, haciendo así a la información aún más valiosa. La toma de decisiones automatizadas a través de la minería de datos y los algoritmos es posible cada vez en más contextos.

El fenómeno de *big data*, denominación que se utiliza para referirse a enormes cantidades de datos que pueden ser almacenados, unidos y analizados, trae consigo la posibilidad de encontrar información, tendencias y conocimientos que no hubieran resultado obvios o a los que no se hubiese podido llegar.

A esto se puede agregar las redes de sensores inalámbricos, que permiten la interacción entre los

individuos o las computadoras y el ambiente que los rodea. Estas redes han tenido mayor desarrollo en áreas tales como la asistencia médica, el medio ambiente, el sistema de transporte, el desarrollo de sistemas de control de energía.

La identificación por radio frecuencia (RFID por sus siglas en inglés) permite la recolección inalámbrica de datos a través de lectores que identifican etiquetas electrónicas (*tags*) adjuntas o embebidas en los objetos, sea para identificación u otros propósitos. El uso de sistemas de RFID requiere componentes de software, redes y bases de datos que permiten que la información se transfiera desde las etiquetas hasta la infraestructura de información de la organización que usa FRID, donde es procesada y almacenada. RFID puede ser utilizado para tarjetas de transporte o de identificación o pasaportes o para compraventa comercial, los usos son muy variados. Las etiquetas electrónicas pueden contener datos personales y dependiendo de la fuerza del lector y de los tipos de protecciones que se apliquen a los datos, éstos pueden ser leídos lo cual, dependiendo de la aplicación y su configuración, pueden llegar a exponer información personal a terceros.

Los dispositivos móviles, sea a través del Sistema de Posicionamiento Global (GPS por sus siglas en inglés) o del uso de software más sofisticado, pueden brindar información acerca del paradero de un individuo y de sus movimientos, permitiendo así el desarrollo de servicios personalizados y a medida, y también publicidad dirigida. La combinación de diversas fuentes de información, como los dispositivos móviles, los RFID habilitados en tarjetas de transporte, las cámaras de vigilancia y otras fuentes de datos de localización, si se combinan, pueden brindar un registro de las localizaciones del individuo y de sus hábitos.

También ha sido notorio el desarrollo tecnológico que permite tomar al cuerpo humano como fuente de información. De tal suerte, los avances en tecnología genética para la prevención y tratamiento de enfermedades, para estimar riesgos para la salud o para establecer lazos biológicos han sido significativos. También los datos biométricos han comenzado a ser recolectados y usados en una cada vez mayor variedad de contextos, principalmente como medio de identificación y autenticación.

iii Cambios en las prácticas organizacionales

También resulta de interés para comprender el actual contexto, mencionar alguno de los cambios identificados por la OCDE en el documento citado, y que se han producido en las prácticas del sector privado, del sector público y de los propios individuos, a partir de las circunstancias mencionadas anteriormente.

El sector privado ha cambiado su modelo de negocios. Las transferencias internacionales de datos en sectores como el de recursos humanos, servicios financieros, educación, comercio electrónico, son parte integral de la economía global. Las transferencias de datos son prácticamente instantáneas

y sin costo, bastando con apretar una tecla o hacer un *click* en el *mouse*[2], para mover los datos rápido y fácilmente alrededor del mundo. El resultado general es que las organizaciones tienen mayor flexibilidad, movibilidad y capacidad de almacenamiento, además de reducir costos. Y esto no sólo para las grandes organizaciones multinacionales, sino también para las pequeñas y medianas organizaciones, y asimismo para individuos, que pueden utilizar servicios globales de almacenamiento, tratamiento y transferencia de datos, que muchas veces involucran a diversos prestadores.

Se han generado también nuevos modelos de negocio basados exclusivamente en los datos personales. La tecnología ha permitido a los individuos compartir información personal muy fácilmente y hay organizaciones que proveen plataformas para contenido generado por el usuario, por lo general sin costo directo, y que buscan generar ingresos con el uso de la información personal del usuario. La perfilería (*profiling*), la selección de sujetos por su conducta (*behavioural targeting*) y la segmentación de audiencias ocurren cada vez a mayor escala.

El sector público también ha utilizado los cambios tecnológicos para cumplir con o mejorar la provisión de determinados servicios y operaciones, a través de un procesamiento de datos personales más eficiente. A su vez, hubo cambios en el modo en que el sector público utiliza internet para informar y comprometer al público, pudiendo acceder de tal forma a datos personales; así, diversas agencias de gobierno o autoridades de aplicación utilizan las redes sociales para buscar participación de los individuos en las políticas públicas.

El sector público ha comenzado a solicitar o requerir al sector privado la retención y entrega de información personal determinada, sea a través de una orden legal o con fines de política pública.

Por último, cabe destacar los cambios en las prácticas que desarrollaron los propios individuos, ya que cada vez más personas realizan transacciones comerciales en línea, incluyendo compras, transacciones bancarias y de viajes. En cada una de estas transacciones, el individuo comparte mucha información personal con las organizaciones con las que interactúa.

Asimismo, el desarrollo de diversas aplicaciones ha permitido que los individuos generen y compartan información, por lo general información personal, pero muchas veces también de familiares y amigos. Las nuevas herramientas y servicios que utilizan los usuarios de internet han generado un cambio en su conducta en línea. Los datos personales son por lo general dados en forma voluntaria por los individuos, sin que sean directamente solicitados por las organizaciones. Muchísimos individuos participan o tienen sus propios blogs[3] comparten fotos y videos en línea, realizan operaciones comerciales entre ellos, e interactúan en grandes grupos de amigos o grupos públicos en sitios de redes sociales.

[2] Mouse o ratón, es un dispositivo de la computadora que se maneja con una sola mano y permite dirigir el movimiento del puntero sobre la pantalla para trasmitir órdenes diversas.

[3] Blog es una página web, generalmente de carácter personal, con estructura cronológica que se actualiza regularmente y que se suele dedicar a un tema en concreto.

III Directrices y principios internacionales

La complejidad y el cambio abrupto que genera el desarrollo tecnológico y el rol estratégico que en este contexto han adquirido (y seguirán teniendo) los datos personales han generado asimismo una serie de preocupaciones vinculadas al riesgo de vulneración de derechos esenciales de los individuos, principalmente el derecho a la privacidad y la autodeterminación informativa, pero también a derechos como la no discriminación, la libertad de expresión, pensamiento y opinión, la libertad de reunión.

Así y haciéndose eco de estas preocupaciones, diversos organismos o instancias internacionales, tanto con vocación global como regional, y tanto de representación gubernamental, como también de representación técnica e inclusive de sociedad civil han generado instrumentos diversos para atender a esta preocupación.

Esos instrumentos son de diverso tipo y alcance, en la mayoría de los casos están presentados como guías o principios sugeridos o propuestos, y en algún otro caso como legislación de aplicación directa. Cabe resaltar asimismo que estos instrumentos buscan armonizar y ponderar el impacto de uno o varios de los derechos mencionados con otros intereses, vinculados a su propia esfera de acción.

Como ejemplo de principios y guías elaborados como propuestas o sugerencias a ser implementados por actores determinados, según el tipo de organización de que se trate, pueden mencionarse de modo no exhaustivo:

- Directrices concernientes a Archivos Computarizados de Datos Personales adoptada por resolución por la Asamblea General de la Organización de las Naciones Unidas.[4]
- Resolución sobre Privacidad en la Era Digital adoptada por la Asamblea General de la Organización de las Naciones Unidas en 2016,[5] que modificó y actualizó posicionamientos anteriores.
- Directrices sobre la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de la Organización para la Cooperación y Desarrollo Económico (OCDE), que fueron inicialmente publicadas en el año 1980 y actualizadas en el año 2013.[6]
- Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, adoptadas por el Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA).[7]

[4] Accesible en http://www.un.org/documents/ga/res/45/a45r095.htm

[5] Accesible en http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

[6] Accesible en http://bit.ly/1Ot27bJ

[7] Accesible en http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

- Marco de Privacidad para la organización internacional de Cooperación Económica de Asia-Pacífico (APEC por sus siglas en inglés).[8]
- Consideraciones de Privacidad para Protocolos de Internet, Pedido de Comentarios N° 6973 (RFC por sus siglas en inglés) del Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés).[9]
- Estándares Internacionales sobre Protección de Datos Personales y Privacidad adoptadas en la 30° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.[10]
- Estándares de Privacidad en un Mundo Global, Declaración de la Sociedad Civil del 3 de noviembre de 2009 en Madrid, España.[11]

IV Distinción entre privacidad y datos personales. El reglamento general de protección de datos personales europeo

No se hará mención en este trabajo de los diversos tratados internacionales[12] que contienen previsiones relativas a la privacidad o protección de datos personales, pues el estudio de los mismos en investigaciones vinculadas a esta materia es profusa.

Sin embargo, sí resulta conveniente aclarar que en Europa, el derecho a la protección de los datos personales tiene reconocimiento legal como derecho distinto al derecho a la privacidad. Varias constituciones nacionales contienen previsiones distintivas en este sentido y, más aún, la Carta de los Derechos Fundamentales de la Unión Europea, adoptada el 7 de diciembre de 2000, establece una clara distinción entre uno y otro derecho. Mientras que el artículo siete consagra el derecho la vida privada y familiar, el artículo ocho reconoce que toda persona tiene derecho a la protección de los datos personales que le conciernan.[13]

Luego, y sin pretender efectuar un análisis de la dinámica normativa de la Unión Europea y/o el Consejo de Europa entre sí y con sus Estados miembros, será tomado como ejemplo de normativa de aplicación directa el Reglamento General de Protección de Datos, dictado por el Parlamento

[8] Accesible en http://bit.ly/1zRV0QK

[9] Accesible en https://tools.ietf.org/html/rfc6973

[10] Accesible en http://bit.ly/2kMYwZA

[11] Accesible en http://thepublicvoice.org/madrid-declaration/es/

[12] Como ejemplo se enumera a la Convención Americana sobre Derechos Humanos, el Pacto Internacional sobre Derechos Civiles y Políticos, el Convenio de Europa sobre Derechos Humanos o el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

[13] Accesible en http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Europeo y el Consejo de Europa el 27 de abril de 2016. Este Reglamento (UE) N° 2016/679[14] es 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.

El Reglamento, que si bien ya está en vigor, será aplicable a partir del 25 de mayo de 2018 en todos los países que integran la Unión Europea (UE) y resulta superador -en tanto aplicación y garantías vinculadas a la autodeterminación informativa y protección de datos personales- de la anterior Directiva 95/46/CE, a la que deroga. Entre varias razones, la adopción del Reglamento respondió también a los cambios descriptos en el apartado 2.1.-

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental para la UE, que asimismo entiende que el tratamiento de datos personales debe estar concebido para servir a la humanidad. Considera también que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación a su función en la sociedad y mantener un equilibrio con otros derechos fundamentales, conforme el principio de proporcionalidad. El Reglamento, tal como se consigna en sus considerandos, respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, en particular el respeto a la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.[15]

El aumento sustancial en los flujos transfronterizos de datos personales motivado en la mayor integración económica y social resultante del funcionamiento del mercado interior, como así también el incremento dentro de la UE del intercambio de datos entre los operadores públicos y privados, incluyendo a las personas físicas, asociaciones y empresas; resalta la relevancia de la generación de la confianza necesaria para el desarrollo de la economía digital en el mercado interior. Asimismo, se debe garantizar un nivel uniforme y elevado de protección para las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la UE y para ello, el nivel de protección de los derechos y libertades de las personas físicas referidas al tratamiento de dichos datos debe ser equivalente, mediante normativa coherente y homogénea.[16]

La anterior Directiva 95/46/CE, vigente durante 20 años, permitió a la UE recorrer un largo camino en materia de protección de datos personales, con organismos y entidades dedicadas exclusivamente al análisis, estudio y resolución de cuestiones vinculadas, como el Grupo de Trabajo del Artículo 29[17]

[14] Accesible en http://bit.ly/2jRVq5P

[15] Ver considerando (4) del Reglamento (UE) 2016/679

[16] Ver considerando (5), (7) y (10) del Reglamento (UE) 2016/679

[17] http://bit.ly/2gs7BE2

o el Organismo Supervisor de Protección de Datos Europeo.[18]

El Reglamento 2016/679 (UE) tendrá alcance más allá de sus fronteras. Por un lado, afecta a empresas que, aunque no tengan establecimiento en la UE, ofrezcan sus productos allí. Por otro lado, el Reglamento dispone la revisión periódica de la adecuación[19] otorgada por la Comisión Europea a terceros países que reciben transferencias de datos desde la UE.

Sin perjuicio de ello y a pesar de encontrarse pendiente su plena implementación, el Reglamento resulta ser un valioso ejemplo en cuanto a su finalidad de armonización normativa supranacional de aplicación directa y al fuerte otorgamiento de garantías y protección de derechos humanos con especial hincapié, claro está, en la autodeterminación informativa, que garantiza a las personas físicas tener el control de sus propios datos personales.

V Normativas nacionales: La situación en Latinoamérica

i Características generales

Siguiendo a Cerda Silva,[20] los sistemas legales latinoamericanos, en tanto comparten la tradición del derecho civil continental europeo, han reconocido también como entidades legales diferentes, el derecho a la privacidad y el derecho a la protección de los datos personales.

El derecho a la protección de datos tiene reconocimiento constitucional. En general, las constituciones de la región reconocen el derecho a la privacidad, pero también incluyen el llamado recurso de *habeas data*, que es el derecho a la protección de los datos personales, tal el caso de las constituciones de Argentina, Brasil, Colombia, México, Perú y Venezuela. Pero aun cuando esta previsión no esté contenida en forma expresa en los textos constitucionales, las Cortes pertinentes han reconocido el derecho de control de la propia información.

Así, el autor destaca que el constitucionalismo latinoamericano ha sido, comparativamente, más eficiente en la protección del derecho a la protección de los datos personales, e identifica tres elementos:

- el reconocimiento del derecho a la protección de datos personales como derecho autónomo;
- el otorgamiento de remedios constitucionales para dicha protección;

[18] http://bit.ly/2kojbWg

[19] La adecuación otogada por la Comisión Europea implica que el país que la recibe tiene protección adecuada de los datos personales; tal el caso de Argentina y Uruguay, entre otros.

[20] Hacia una Internet Libre de Censura: propuestas para América Latina. Capítulo 4. Protección de datos personales y prestación de servicios en línea en América Latina. Autor: Alberto Cerda Silva. Compilador: Eduardo Bertoni. Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. Accesible en http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

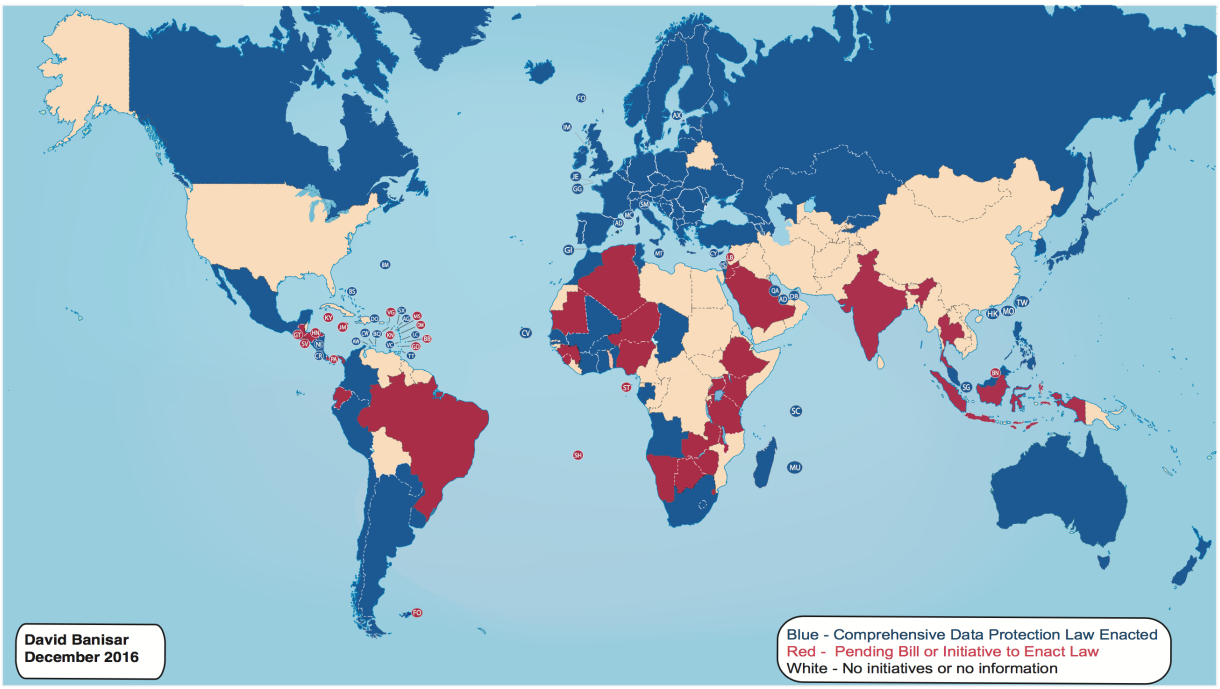
- y siguiendo aún más la tradición constitucional europea, mediante el reconocimiento de derecho y otorgamiento de acciones no sólo respecto del sector público, sino también contra actores no estatales.

Sin embargo, la protección constitucional no es suficiente, debido a causas bastante comunes en la región, por ejemplo: los altos costos transaccionales, la ineficiencia en la prevención del incumplimiento, la falta de *stare decisis* de las decisiones judiciales -ya que, salvo contadas excepciones, sólo aplican al caso sujeto a decisión judicial. A eso puede agregarse que las previsiones constitucionales son muy generales, dejando así mucho margen para la interpretación judicial, por lo que al ser aplicados a casos concretos pueden generarse decisiones ambiguas o equivocadas, generando así falta de certeza legal.

América Latina en general ha adoptado mayormente durante la década de 1990 leyes comprensivas para el procesamiento de datos personales, es decir, leyes que regulan el procesamiento automático y manual de datos personales tanto por el sector público como por el sector privado. De tal suerte ha seguido también la tradición europea de protección comprensiva, a diferencia por ejemplo de los Estados Unidos, cuya protección es fragmentada por sector y se basa, muy sucintamente, en criterios de privacidad y datos de alta sensibilidad, no en la autodeterminación informativa.

El siguiente mapa elaborado por David Banisar[21] permite observar (en azul) los países que cuentan con leyes comprensivas de protección de datos en América Latina y el resto del mundo.

National Comprehensive Data Protection/Privacy Laws and Bills 2016



[21] Banisar, David, Leyes y Proyectos de Leyes Nacionales Comprensivas de Protección de Datos Personales y Privacidad 2016. Disponible en SSRN: https://ssrn.com/abstract=1951416 o http://dx.doi.org/10.2139/ssrn.1951416

En su trabajo, Cerda Silva señalaba que el modelo de protección de datos personales latinoamericano se encuentra en una fase de transición. La mayor parte de las principales economías de la región cuentan con protecciones constitucionales y leyes comprensivas de protección que regulan el procesamiento de datos personales tanto por el sector público como el privado.

Así y en rasgos generales, la protección de datos personales en América Latina aparece como robusta. Sin embargo, los países todavía necesitan trabajar para que estas leyes sean de aplicación efectiva y respondan a los actuales desafíos generados por el desarrollo tecnológico y la cada vez más creciente transferencia internacional de datos personales.

ii Análisis comparativo de cuatro países de la región: Argentina, Chile, Brasil y México. Su correspondencia con estándares internacionales

i Consideraciones preliminares

Lo reseñado en el apartado precedente será ilustrado a partir del análisis comparativo de los sistemas de protección de datos personales de cuatro países de la región, a saber: Argentina, Chile, Brasil y México. Los últimos tres países fueron seleccionados por encontrarse en procesos de reforma de su normativa.

El análisis incluirá la correspondencia de las características de cada uno de estos sistemas con los estándares propugnados por el sistema europeo de protección de datos personales.

A su vez, la elección del sistema europeo como referencia internacional se basó en varios motivos, entre ellos:

- las legislaciones latinoamericanas se han desarrollado mayormente siguiendo la inspiración del sistema continental europeo;
- los países de la región han adoptado, en consonancia con el sistema europeo, la distinción entre derecho a la privacidad y el derecho a la autodeterminación informativa, como figuras legales diferenciadas;
- el sistema europeo de protección de datos personales tiene vocación armonizadora y contiene marcadas referencias a la protección de otros derechos humanos, la ponderación entre los mismos, y el libre flujo de datos tendiente a posibilitar el desarrollo de la economía digital;
- varios de los países de la región han adoptado sistemas de protección inspirados en la normativa europea, en particular la normativa española;

- desde el año 2003 funciona la Red Iberoamericana de Protección de Datos Personales,[22] que nuclea a los organismos de protección de datos personales o con vocación similar de los países iberoamericanos y que entre múltiples actividades, ha celebrado 15 encuentros anuales. Además de España, entre miembros y observadores, tienen participación en dicha red 14 países de Latinoamérica, además de participar como observadores el Supervisor Europeo de Protección de Datos Personales en representación de la Unión Europea, entre otros organismos internacionales;

- al menos dos países de la región (Argentina[23] y Uruguay[24]) han sido declarados países adecuados por la Comisión Europea, por tanto sus sistemas de protección de datos personales ya se encuentran alineados con los estándares europeos previstos inicialmente por la anterior Directiva 95/46/CE;

- a mayor abundamiento, Uruguay ha formalizado su adhesión al Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal en agosto de 2013.

Para el cabal conocimiento de la situación de cada uno de los países seleccionados, se contó con el invaluable aporte de colegas de organizaciones de sociedad civil, que durante 2015 y 2016 efectuaron sendos análisis de sus normativas internas y su correspondencia con los estándares europeos.

De tal suerte, las organizaciones que elaboraron tales reportes fueron Derechos Digitales para Chile, InternetLab para Brasil, Red en Defensa de los Derechos Digitales para México, y el del Argentina fue realizado por Eduardo Ferreyra de Asociación por los Derechos Civiles.

Por último, merece un comentario aparte la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas, adoptadas en 2012 por el Comité Jurídico Interamericano de la Organización de Estados Americanos (OEA).[25] En este sentido, si bien dichos principios pretenden guiar el desarrollo de los sistemas legales de protección de datos personales de los países que integran la OEA, que obviamente incluye a los países de Latinoamérica, cabe decir que los mismos no fueron tenidos como referencia de estándares internacionales para la comparación que aquí se pretende realizar. Ello así toda vez que los principios adoptados por el Comité Jurídico establecen una línea muy baja de protección, quedando por debajo de los sistemas vigentes en varios países de la región y muy lejanos a los estándares de protección de datos personales propiciado por el sistema europeo, cuyas características ya se han señalado.

[22] Ver Red Iberoamericana de Protección de Datos Personales en http://www.redipd.es/index-ides-idphp.php
[23] Decisión UE 2003/490 de la Comisión Europea del 30 de junio de 2003. Accesible en http://bit.ly/2kReKzZ
[24] Decisión UE 2012/484 de la Comisión Europea del 21 de agosto de 2012. Accesible en http://bit.ly/2jrETJF
[25] Accesible en http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

ii Metodología

Para la comparación se utilizó como fuente los reportes de cada país, cuya lectura se sugiere dado la riqueza de los mismos y para la cabal comprensión de la información que se brindará en los próximos títulos. Los reportes fueron elaborados entre 2015 y 2016.

- El reporte de Argentina se encuentra disponible aquí
- El reporte de Chile se encuentra disponible aquí
- El reporte de México se encuentra disponible aquí
- El reporte de Brasil se encuentra disponible aquí (en idioma inglés)

Luego de un breve análisis de las características principales de los marcos normativos de cada país, se abordará cada uno de los siguientes elementos: definiciones; principios relativos al tratamiento de datos, consentimiento; derechos del titular de los datos o interesado; responsabilidad y obligaciones del usuario de los datos y demás sujetos vinculados; transferencia y cesión; mecanismos para la aplicación y cumplimiento (*enforcement*) como autoridad de aplicación y control, sanciones, acciones en cabeza del titular y compensación por daños y perjuicios.

Respecto de cada elemento reseñado, se resaltarán las características principales de cada uno de acuerdo al sistema europeo,[26] y se destacarán los rasgos sobresalientes de los países en análisis. Cuando sea pertinente, cada elemento será ilustrado con una tabla comparativa de los cuatro países.

Se destaca que los aspectos seleccionados tienen a abarcar supuestos generales, por lo que en el análisis siguiente no se encontrarán menciones al tratamiento particular de determinados datos, como los datos sensibles, los financieros, los de publicidad, los que se encuentren en poder de la policía y fuerzas de seguridad, etc.

ii.1 Marco normativo Los cuatro países bajo análisis consagran en sus constituciones el derecho a la privacidad y tres de ellos contienen previsiones relativas al derecho a la protección de datos personales, Argentina y Brasil en tanto se refieren al *habeas data* (acción de protección de datos) y México como derecho en sí mismo. Por su parte Chile, si bien no lo menciona en forma expresa, ha generado una alternativa de reconocimiento de datos personales como figura separada del derecho a la privacidad a través del accionar jurisprudencial.

Argentina, Chile y México cuentan con leyes comprensivas de protección de datos personales. La ley argentina data del año 2000 y la chilena fue sancionada en el año 1996. A mayor abundamiento,

[26] El Reglamento General de Protección de Datos europea N° 2016/279. Accesible en http://bit.ly/2kdyleT

México cuenta con una ley específica para el sector privado del año 2010 y una ley aprobada recientemente (diciembre 2016) específica para el sector público.

Brasil no cuenta con una ley específica para la materia ni con un sistema de protección de datos personales. Sin embargo pueden encontrarse algunas previsiones relativas a diversos tipos de datos personales en distintas leyes y normativa. Así se identifican referencias a la protección de datos de las telecomunicaciones, en la Ley General de Telecomunicaciones, resoluciones de Anatel (ente regulador de las telecomunicaciones), el Marco Civil de Internet y su decreto reglamentario, ley de interceptaciones, ley de organizaciones criminales y código Penal como marco referencial. También se encuentra referencias relativas a datos de los consumidores, de los datos financieros y de datos de salud en normativa específica de cada uno de estos sectores.

Cabe agregar que Argentina se encuentra en un proceso de reflexión para la reforma de la ley vigente[27] y que Chile está a la espera de la anunciada presentación por parte del gobierno de un proyecto de ley integral, comprensivo y superador de la deficitaria ley vigente, sin perjuicio de haberse presentado en el Parlamento diversos proyectos de ley, que en su mayoría apuntan a aspectos particulares y determinados, por lo que adolecen de una visión integral del sistema de protección de datos.

Brasil también ha dado cuenta de la necesidad de una ley comprensiva de protección de datos, y mediante un proceso de participación colectiva iniciado por el Ministerio de Justicia fue elaborado un proyecto de ley, N° 5276 de 2016, que fue presentado al Congreso en el mes de mayo de ese año. Dado la trascendencia de este proyecto, será mencionado en los puntos siguientes.

Marco normativo	**Argentina**	**Chile**	**México**	**Brasil**
Constitución Nacional				
Privacidad	+	+	+	+
Datos personales/habeas data	+	–	+	+
Ley de PDP	+	+	+ (2)	–

Tabla 5.1.- Comparativa del Marco Normativo[28]

ii.2 Definiciones El Reglamento General de Protección de Datos europeo (RGPD) contiene un amplio catálogo de definiciones acerca de conceptos que son considerados decisivos para la regulación del tratamiento de datos personales y que reflejan, de algún modo, la complejidad actual de las diversas variables que interactúan en el tratamiento de datos personales, como la multiplicidad de sujetos, los diversos tipos de datos y el entorno tecnológico.

[27] http://www.jus.gob.ar/datos-personales/comunicados/2016/12/19/aportes-sobre-la-necesidad-de-una-reforma-a-la-ley-sobre-proteccion-de-los-datos-personales-(1).aspx

[28] Tabla comparativa de elaboración propia.

En este sentido, la lista es mucho más larga que la prevista por las leyes Argentina y Chile, que se ciñen a una modesta lista de conceptos que cubre mayormente definiciones vinculadas a los sujetos y tratamiento de datos. Sin embargo y en líneas generales, las definiciones contenidas en las leyes guardan características similares. La excepción es México, cuya normativa contiene una larga lista de definiciones, incluyendo términos como "cómputo en la nube" y otros de tenor más bien tecnológico.

A modo ilustrativo, entre los conceptos incorporados por el Reglamento y que no figuran en las leyes vigentes de los países en estudio (con excepción de México que en algunos casos los considera), se cuentan: limitación de tratamiento, elaboración de perfiles, datos genéticos, datos biométricos, empresa, grupo empresarial, normas corporativas vinculantes, servicio de la sociedad de la información.

A renglón seguido, serán brevemente analizado cuatro definiciones en particular: datos personales, datos sensibles, tratamiento, titular.

En relación al concepto de datos personales, Argentina, Chile y México comparten definiciones similares, en tanto se refieren a los datos de personas físicas identificadas o identificables (Argentina también incluye a las personas de existencia ideal).

Esta noción guarda relación con la propuesta en el RGPD. Sin embargo, la definición de datos personales del Reglamento va más allá y establece que una persona se considerará identificable cuando su identidad pueda "determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

La legislación sectorizada de Brasil carece de una definición de datos personales a pesar de encontrarse mencionada en diversa normativa (como el Marco Civil de Internet). El proyecto de ley 5276/2016 intenta subsanar esta omisión, de modo similar al propiciado por el RGPD.

Respecto a los datos sensibles, los cuatro países en análisis contienen una definición similar, que puede considerarse alineada con las previsiones del RGPD. El Reglamento -que se refiere a los datos sensibles como "categorías especiales de tratamiento de datos"- incluye varios datos ya previstos por las leyes de los países en cuestión, a saber: datos que revelen origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, los datos relativos a la salud o a la vida sexual de las personas. Sin embargo, incorpora algunos tipos de datos como los datos genéticos (incluido también en la normativa mexicana) y los datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Cabe destacar que en el caso de Brasil, la definición de datos sensibles se encuentra en la Ley de Registros Financieros. Por su parte, el proyecto de ley 5276/2016 incorpora una definición alineada al Reglamento.

En cuanto al tratamiento, cabe destacar que también hay bastante coincidencia en cuanto a las actividades englobadas en el concepto de "tratamiento", en tanto alude a cualquier operación o

conjunto de operaciones, sea por procedimientos automatizados o no, y que van desde la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, transmisión, cesión, etc. Las leyes de Argentina, Chile y México contienen la definición de tratamiento; no así Brasil, aunque sí el proyecto 5276/2016.

Respecto del titular –denominado "interesado" en el RGPD- también hay coincidencia en tanto se trata de toda persona física o natural de cuyos datos se trate. También puede inferirse este criterio en Brasil, en virtud de la definición de datos sensibles que contiene la ley de registros financieros, que además es recogido por el proyecto de ley 5276/2016. La excepción está dada por Argentina, que también incluye a las personas de existencia ideal o física.

Definiciones	**Argentina**	**Chile**	**México**	**Brasil**
Dato personal	+	+	+	–
Dato sensible	+	+	+	+/- (*)
Tratamiento	+	+	+	–
Titular	+	+	+	–

Tabla 5.2.- Comparativa de definiciones. (*)Aquí se utilizó +/- dado que la definición de dato sensible surge de una ley que rige para un sector específico, y no con alcance general.[29]

ii.3 Principios relativos al tratamiento de datos personales El RGPD contiene una serie de principios que deberán observarse en todo tratamiento de datos.

- licitud, lealtad y transparencia: los datos deberán tratados de manera lícita, leal y transparente en relación con el interesado. Debe entenderse por lícito que el tratamiento se ajuste a lo previsto en la ley y por "transparente" toda la información que se le debe suministrar el titular en ocasión de la recolección de los datos, vinculada a quién es el responsable y su domicilio, qué se harán con los datos y sus posibles destinatarios, carácter facultativo u obligatorio y las consecuencias de proporcionar o no los datos, la posibilidad de ejercer determinados derechos, etc.;

- limitación de la finalidad: los datos deberán ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines. El tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales;

[29] Tabla comparativa de elaboración propia.

- exactitud: los datos deberán ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan;
- limitación del plazo de conservación: los datos deberán ser mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos;
- integridad y confidencialidad: los datos deberán ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas;
- minimización de datos: los datos deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Tomando en consideración la normativa argentina, existe una relativa similitud entre los principios consagrados en ambas legislaciones. Así, los dos ordenamientos reconocen los principios de licitud, transparencia, finalidad, exactitud, necesidad, confidencialidad y limitación del plazo de conservación. Sin embargo, las diferencias surgen al momento de determinar el contenido de cada uno de ellos. Por ejemplo, mientras que para la ley argentina el principio de licitud se cumple cuando la base de datos se encuentra inscripta en el Registro creado a tal efecto, además de observar los principios establecidos en la ley. Por su parte el RGPD en su artículo establece una serie detallada y precisa de condiciones las cuales -al menos una- deben ser cumplidas para ser considerado lícito el tratamiento, entre las que no está contemplado el registro de las bases.

Por su parte, la legislación chilena no hace un listado explícito de los principios aplicables a las operaciones de tratamiento de datos. Sin embargo, de las disposiciones de la ley se pueden deducir al menos tres: el principio de finalidad, el principio de calidad de los datos y el principio de licitud.

La legislación mexicana consagra los principios de licitud y lealtad, consentimiento, finalidad, proporcionalidad, calidad, responsabilidad e información. El "aviso de privacidad" es uno de los elementos más importantes del esquema previsto en la normativa, y consiste en documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales (para el sector privado) o a partir del momento en el cual se recaben sus datos personales (para el sector público), con el objeto de informarle los propósitos del tratamiento de los mismos

En el caso de Brasil, es el Marco Civil de internet que establece dos principios para el tratamiento de datos: el principio de transparencia y el principio de finalidad. El Decreto Reglamentario del Marco

Civil incluye una mención al principio de minimización y de limitación en el plazo de conservación. El mentado proyecto de ley 5276/2016 ofrece una serie de principios alineados con la normativa europea.

Los principios de minimización y de responsabilidad proactiva no aparecen como tales en los textos normativos en estudio, con excepción de lo mencionado en el apartado anterior.

Principios	**Argentina**	**Chile**	**México**	**Brasil**
Licitud, lealtad y transparencia	+	+	+	+/-(*)
Limitación de la finalidad	+	+	+	+/-(*)
Exactitud	+	+	+	–
Limitación en el plazo de conservación	+	–	+	+/-(*)
Integridad y confidencialidad	+	–	+	–

Tabla 5.3.- Comparativa de Principios. (*)Aquí se utilizó +/- dado que la definición de los principios en cuestión fueron detectados en el Marco Civil de Internet, que no es una ley de protección de datos personales.[30]

Cabe dedicar unas breves palabras en relación al requisito de registro de las bases de datos, que por ejemplo en Argentina es necesario para la licitud del tratamiento, por lo deben registrarse todas las bases de datos, sean públicas o privadas. Chile sí establece el registro de sus bases públicas. Se aclara que la legislación mexicana contempla la creación de un Registro Nacional de Protección de Datos[31] para los organismos públicos, pero dicha medida no se refiere al registro de las bases de datos públicos, sino al registro de los esquemas de mejores prácticas implementadas por los organismos, con el objeto de transparentar y hacer del conocimiento del público en general los procedimientos para garantizar el derecho de las personas para la protección de los datos, independientemente del nivel de gobierno y a través.

Registro	**Argentina**	**Chile**	**México**	**Brasil**
Bases de datos públicas	+	+	–	–
Bases de datos privadas	+	–	–	–

Tabla 5.4.- Comparativa de Registro de Bases.[32]

ii.4 Consentimiento En el RGPD el consentimiento constituye una de los supuestos por los cuales se considera lícito el tratamiento de datos. Esto significa que si bien es uno de los más importantes, el consentimiento no tiene una preeminencia en el sistema de protección de datos de

[30] Tabla comparativa de elaboración propia.

[31] Ver en http://registronacional.com/mexico/registro-nacional-de-proteccion-de-datos.htm

[32] Tabla comparativa de elaboración propia.

la UE sino que coexiste con otras supuestos legítimos establecidos por la legislación, a saber: si es necesario para la ejecución de un contrato en la que el interesado es parte; si es necesario para el cumplimiento de una obligación legal del responsable del tratamiento; si es necesario para proteger intereses vitales del interesado u otra persona física; si es necesario para el cumplimiento de una misión de interés público o en ejercicio de poderes públicos; y si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, en tanto no prevalezcan los intereses o los derechos del interesado.

Por el contrario, en la legislación argentina el consentimiento es la regla general para la licitud de todo tratamiento de datos personales y los casos en los que no se necesita dicho consentimiento están configurados como excepciones a dicha regla. La ley argentina establece como regla general que todo tratamiento de datos debe realizarse con el consentimiento libre, expreso e informado del titular; de acuerdo a las circunstancias, deberá ser hecho por escrito o por un medio que se lo equipare. Así, el consentimiento tácito o presunto no es considerado válido por la ley, aunque dicha regla tiene excepciones.

Por su parte, la ley Chilena establece que el consentimiento del titular de los datos es necesario para el tratamiento de sus datos, salvo que una disposición legal lo haya autorizado. La normativa establece que el consentimiento desde ser expreso, informado y por escrito; y también contiene los casos en que el consentimiento estará exceptuado. En México, como regla general, los datos personales sólo podrán ser tratados con el consentimiento de su titular, obtenido de manera libre, específica e informada. El consentimiento deberá ser expreso si se trata de datos personales sensibles y financieros o patrimoniales.

En Brasil varias disposiciones sectoriales requieren el consentimiento expreso del titular. Así surge de la Ley General de Telecomunicaciones, del Código de Protección del Consumidor y del Marco Civil de Internet.

Al momento de definir el consentimiento, el Reglamento afirma que es una "manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". De esta manera, la normativa europea no utiliza el calificativo "expreso" presente en las legislaciones en estudio y admite además de una declaración, la presencia de otras "acciones afirmativas claras" que sean expresión del consentimiento del interesado.

Todas las legislaciones prevén diversos supuestos de revocación del consentimiento.

Resulta interesante traer un aspecto resaltado por los colegas de Brasil en su reporte, relativo a la figura del "interés legítimo" contenida en la normativa europea (ver más arriba), toda vez que ha sido materia de especial discusión en el proceso legislativo relativo al proyecto de la ley 5276/2016. Es así como en el mentado proyecto el consentimiento sigue siendo un requisito de licitud, en tanto sea libre, informado e inequívoco. Asimismo, en dicho proyecto se incluyó como otra hipótesis

de licitud la del interés legítimo del responsable del procesamiento de la información en ciertas situaciones en las que el consentimiento explícito del interesado no se considera necesario. Dicho en otras palabras, si el responsable tiene un interés legítimo en el tratamiento de la información no sería necesario obtener el consentimiento del interesado.

Esta provisión relativa al interés legítimo despertó en Brasil la preocupación de diversos actores ya que, por un lado, se hizo notar que esta figura reconoce que otras partes distintas al titular de los datos puedan tener intereses legítimos en el procesamiento, uso o transferencia de determinada información. Además, permite sobrellevar circunstancias en las que no es posible obtener el consentimiento del titular y el ejercicio de derechos o la prevención de daños dependen del procesamiento de sus datos.

Pero, por otro lado, también se resaltó que el interés legítimo puede llegar a interpretarse como una excepción que permite una autorización general para todo tipo de tratamientos con cualquier tipo de propósito, sin ningún control o conocimiento por parte del titular de los datos. Por eso se enfatizó en que para establecer un adecuado balance entre la protección a la privacidad y la intimidad y el desarrollo económico y la innovación, debería contemplarse la inclusión de muy claros límites para el uso del interés legítimo como base legal para el tratamiento de la información, y así evitar abusos en su utilización.

ii.5 Derechos del titular Argentina, Chile y México contemplan en sus legislaciones los famosos derechos ARCO, que consisten en:

- Acceso: exigir al responsable de una base de datos información sobre los datos relativos a su persona que se encuentran en dicha base, como por ejemplo su procedencia y destinatario, propósito del almacenamiento, individualización de quienes reciben los datos;
- Rectificación: solicitar al responsable de una base de datos que corrija, actualice o modifique los datos si así correspondiese, por ser inexactos, erróneos, equívocos o incompletos.
- Cancelación: solicitar la eliminación del dato cuando el almacenamiento carezca del fundamento legal o el dato estuviere caduco.
- Oposición: solicitar la eliminación o bloqueo cuando se haya proporcionado un dato en forma voluntaria, o se usen para comunicaciones comerciales y no se desee seguir figurando en dicha base (cfr. legislación chilena).

El ejercicio de estos derechos tiene excepciones, como por ejemplo las que establece la legislación argentina respecto de la supresión o cancelación, que no podrá tener lugar cuando la medida pudiere afectar derechos o intereses de terceros, o cuando existe una disposición legal de conservar los datos.

Brasil también contiene previsiones relativas a estos derechos, circunscriptas a los ámbitos de aplicación de tales normas. Así, por ejemplo, el Código de Protección al Consumidor de Brasil consagra el derecho de acceso, de rectificación y de cancelación.

El RGPD consagra los derechos tradicionales vinculados a la protección de datos personales, como el derecho a la información, el derecho al acceso, el derecho a la rectificación y el derecho a la oposición. Sin embargo, agrega otros nuevos derechos no previstos -o previstos de manera distinta-en los plexos normativos en análisis (excepto en los casos que se indicarán de modo expreso).

- Derecho a la supresión o "derecho al olvido", por el cual toda persona tiene la facultad de solicitar la supresión de los datos personales que ya no sean necesarios para el cumplimento de las finalidades para las que fueron recogidos, cuando se haya retirado el consentimiento y no exista otra base legal para el tratamiento del mismo, cuando el tratamiento haya sido realizado en forma ilícita, etc. En estos casos, el responsable del tratamiento deberá adoptar medidas razonables, teniendo en cuenta la tecnología disponible y el coste de su aplicación, incluyendo medidas técnicas, con miras a informar a otros responsables de la solicitud de supresión de cualquier enlace a esos datos personales o cualquier copia o réplica de los mismos.

- Derecho a la limitación del tratamiento. En virtud de este derecho, la persona puede solicitar que sus datos sean conservados pero sin que puedan ejercerse otro tipo de tratamiento. Las condiciones en que procede este derecho son: que el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; que el tratamiento sea ilícito y el interesado no solicite la supresión sino su limitación; el responsable ya no necesite los datos personales pero el interesado sí para la formulación, el ejercicio o la defensa de reclamaciones; y cuando el interesado se haya opuesto a un tratamiento de datos, mientras se verifica si los motivos del responsables prevalecen o no sobre los del interesado. En estos casos, el responsable puede trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, impedir el acceso de usuarios a los datos personales seleccionados o retirar temporalmente los datos publicados de un sitio de Internet.

- Derecho a la portabilidad, en virtud del cual toda persona tiene derecho a recibir los datos personales que le incumban que haya facilitado a un responsable del tratamiento y a transferirlos a otro responsable, sin que el anterior pueda impedirlo. El interesado puede pedir la entrega de sus datos en un formato de uso común o lectura mecánica o que directamente se le entregue al nuevo responsable, siempre que sea técnicamente posible. México contiene una previsión relativa a la portabilidad de los datos cuando se trata organismos públicos.

- Derecho a la oposición y marketing directo. En el considerando 47, el Reglamento sostiene que el tratamiento de datos con fines de marketing directo puede considerarse realizado por interés legítimo. Sin embargo, dentro de la normativa, el legislador ha contemplado como un

supuesto especial del derecho a la oposición en caso de estas bases de datos. En ese sentido, se otorga el derecho a las personas a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles. Si el interesado ejerce este derecho, los datos personales deben dejar de ser tratados para estos fines. A fin de facilitar este ejercicio, se consagra la obligación de informar al interesado en la primera comunicación que se mantenga con él de la existencia de este derecho en forma clara y al margen de cualquier otro tipo de información. Chile tiene en su normativa una disposición similar.

- Decisiones individuales automatizadas (art.22): El RGPD consagra el derecho de toda persona a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. De esta manera, se busca garantizar un tratamiento leal y transparente respecto del interesado con el fin de evitar -por dar un ejemplo- decisiones producidas por la utilización de algoritmos que pueden exacerbar los ya existentes patrones sociales de discriminación y exclusión. Argentina tiene una previsión en similar sentido, aplicable al tratamiento realizado por organismos públicos y México también, pero para el sector privado.

En relación a este último derecho incluido en la normativa europea la doctrina[33] ha sostenido que en este supuesto pueden deducirse dos derechos derivados del Reglamento. El primero es el derecho a la no discriminación, mediante el cual las personas tienen el derecho a no verse discriminadas por decisiones algorítmicas basadas en la utilización de datos que revelan prejuicios raciales, sociales, de género o de cualquier otro tipo. El segundo derecho es el derecho a una explicación, que faculta a las personas a solicitar al responsable de un tratamiento de datos que informe acerca de la lógica y el funcionamiento del algoritmo utilizado para sus operaciones. Como bien dice el nombre, este derecho se satisface cuando el proceso es explicado en forma clara y comprensiva para la persona, de manera que ésta pueda evaluar si la toma de decisión ha afectado alguno de sus derechos.

Vale agregar que el proyecto de ley 5276/2016 brasilero contiene previsiones relativas a los derechos ARCO tradicionales en cabeza del titular de los datos, y también previsiones en línea con los nuevos agregados del RGPD.

ii.6 Responsabilidades y obligaciones de quien trata los datos y sujetos vinculados Parte de las normas de los países en estudio, al igual que en RGPD, obligan a los sujetos responsables del tratamiento a la adopción de una serie de medidas. Sirva de aclaración que aquí se ha utilizado sólo un término – responsable del tratamiento-, pero lo que se expresa debe hacerse extensivo a todos los sujetos que intervienen en el procesamiento de datos, conforme establezca cada legislación en particular.

[33] Ver Bryce Goodman y Seth Flaxman "European Union regulations on algorithmic decision-making and a "right to explanation" 2016, Oxford, disponible en https://arxiv.org/pdf/1606.08813v3.pdf

Entre dichas medidas se puede mencionar:

- Implementación de medidas de seguridad de carácter administrativo, físico, técnico y legal para el tratamiento y protección de los datos, que permitan proteger contra daño, pérdida, alteración, destrucción; o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.
- Esquema de mejores prácticas para elevar el nivel de protección, armonizar el tratamiento, capacitación, etc.
- Evaluación de impacto en la protección de datos personales, a fin de valorar los impactos reales de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos.
- Notificación en caso de vulneración de datos, sea al titular y/o a la autoridad de aplicación.
- Procedimiento de verificación para vigilar y verificar el cumplimiento de las disposiciones de protección de datos.

Obligaciones/responsabilidades	**Argentina**	**Chile**	**México**	**Brasil**
Adopción de medidas técnicas	+	−	+	−
Evaluación de Impacto o Riesgo	−	−	+	−
Notificación por vulneración	−	−	+	−
Procedimiento de verificación	−	−	+	−
Esquema de mejores prácticas	−	−	+	−

Tabla 5.5.- Comparativa de obligaciones y responsabilidades.[34]

El RGPD agrega una serie específica de medidas a adoptar, ausente en la legislación en análisis, con excepción de México en algunos supuestos. Así se enumera:

- Registro de actividades de tratamiento que debe ser llevado por cada responsable.
- Privacidad por diseño y privacidad por defecto. La primera consiste en la obligación de todo responsable de tratamiento de aplicar todas las medidas necesarias (seudominización, limitación del tratamiento, etc.) para respetar la privacidad de los usuarios desde el mismo momento en que se determina los medios de tratamiento. De esta manera, todo proveedor de servicio, aplicación o similar debe tomar en cuenta al momento de diseñar su producto la necesidad de que el mismo no afecte los derechos de las personas. Vinculado con esto, se

[34] Tabla comparativa de elaboración propia.

encuentra el deber de garantizar por defecto que todo tratamiento de datos tenga como objeto sólo aquellos necesarios para los fines de su actividad (privacidad por defecto). Asimismo, estas medidas deben garantizar que los datos personales no sean accesibles a un número indeterminado de personas.

- Notificación de una violación de seguridad.
- Evaluación de impacto o riesgo en la protección de datos.
- Delegado de Protección de Datos.

ii.7 Cesión y transferencia internacional Las referencias a estas figuras se encuentran en la legislación mexicana y en la legislación argentina.

En la legislación mexicana la transferencia de los datos a terceros nacionales o extranjeros, distintos del encargado, se hará conforme a lo convenido en el aviso de privacidad, el que contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos; de igual manera, el tercero receptor, asumirá las mismas obligaciones que corresponden al responsable que transfirió los datos.

La ley que afecta a los sujetos obligados del sector público mexicano, establece que toda transferencia se encuentra sujeta al consentimiento del titular y se formalizará mediante instrumentos jurídicos que permitan demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

En Argentina la cesión de datos personales desde una base a otra es permitida, sólo si se cumplen los siguientes requisitos: que la cesión se haya realizado para cumplir fines directamente relacionados con el interés legítimo de cedente y cesionario; que el titular del dato haya dado su consentimiento previo, y que éste haya sido informado de la finalidad de la cesión, y de la identificación del cesionario o de los elementos para poder hacerlo. Si la transferencia se produce, el cesionario quedará sujeto a las mismas obligaciones reglamentarias y legales del cedente, el cual a su vez, deberá responder en forma solidaria y conjunta ante cualquier violación de la legislación. Asimismo, el consentimiento es revocable y el titular puede solicitar en cualquier momento al cesionario que deje de realizar el tratamiento correspondiente.

Sin embargo, la ley argentina establece que el consentimiento para la cesión o transferencia no siempre es necesario. Existen varias excepciones a la regla: cuando lo disponga una ley, cuando se trate de uno de los supuestos por los cuales no es necesario el consentimiento para el tratamiento del dato, cuando se trate de cesiones de datos entre dependencias de los órganos del Estado en forma directa, siempre y cuando se realicen dentro del marco de sus competencias; se trate de datos relativos a la salud, a condición de que sean necesarios por razones de salud pública, emergencia

o para realizar estudios epidemiológicos y se preserve la identidad de los titulares de los datos; y cuando se hubiera aplicado un procedimiento de disociación de la información, de manera que las personas no puedan ser identificadas.

Por su parte, tanto el RGPD como la ley argentina sostienen el principio de que sólo se permitirán transferencias internacionales de datos a aquellos países que cuenten con un nivel adecuado de protección. Al momento de determinar los criterios por los cuales se considera que un país u organización tiene un nivel adecuado, el Reglamento contiene una detallada exposición de los elementos que se deben analizar. Entre ellos figuran: el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes, los compromisos internacionales asumidos, etc. Por el contrario, la ley argentina no contiene una disposición similar. Esta omisión fue atenuada por el decreto reglamentario, que estableció que se debe tener en cuenta la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

En caso de que el país o la organización no cuente con la adecuación, el RGPD prevé la transferencia de datos personales en caso de que el responsable o encargado ofrezca garantías adecuadas, las cuales pueden ser: un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos, normas corporativas vinculantes, cláusulas tipo de protección de datos adoptadas por la Comisión Europea o por una autoridad de control, un código de conducta o mecanismo de certificación.

Si tampoco pueden ofrecerse garantías adecuadas, el RGPD establece una última lista de supuestos en los cuales procede la transferencia, a saber: cuando el interesado (titular) haya dado explícitamente su consentimiento o cuando la transferencia sea necesaria para: la ejecución de un contrato entre el interesado y el responsable del tratamiento; la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica; por razones importantes de interés público: para la formulación, el ejercicio o la defensa de reclamaciones; o para proteger los intereses vitales del interesado o de otras personas.

A diferencia del RGPD, la legislación argentina consagra un corto catálogo de excepciones: colaboración judicial internacional, intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica; transferencias bancarias o bursátiles, cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; o cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. A su vez, el decreto reglamentario agregó el consentimiento expreso del titular de

los datos o interesado y el caso de datos contenidos en registros públicos abiertos a la consulta del público en general.

ii.8 Mecanismos para la aplicación y cumplimiento (enforcement) En este apartado serán analizados los mecanismos de que contienen las legislaciones en análisis para asegurar la efectiva aplicación y cumplimiento de las garantías y protecciones que contienen sus previsiones. A tal efecto, se abordarán cuatro aspectos: a) la autoridad de aplicación y contralor; b) las sanciones y c) las acciones y recursos; d) compensación.

ii.8.1 La autoridad de aplicación y contralor La normativa europea ha sido señera en establecer las pautas que debe cumplir la autoridad estatal de aplicación y contralor que en definitiva se establezca a efectos del adecuado cumplimiento de la normativa, garantizando así el ejercicio del derecho de autodeterminación informativa. En este caso debe aclararse que el RGPD no se aplica en forma directa, sino que son los Estados miembros de la UE -a través de su legislación interna- los encargados de poner en práctica lo dispuesto por la norma comunitaria.

De modo abreviado, el RGPD indica que la autoridad de aplicación y contralor debe contar con independencia funcional y financiera, a fin de poder efectuar libremente los controles que correspondan respecto del tratamiento de datos llevado adelante por el Estado y por los privados. También exige determinados recaudos de idoneidad y establece condiciones para la designación transparente y terminación del mandato del responsable del organismo de aplicación y control. Ello así a fin de evitar la que la designación y el cese del funcionario sean decisiones discrecionales del gobierno de turno.

A su vez, el RGPD establece que el órgano de aplicación deberá contar con facultades de investigación, rectificación, consulta, en todo caso respetando la tutela judicial efectiva (revisión judicial posterior) y las garantías procesales. La facultad de iniciar procedimientos judiciales dependerá de la normativa interna de cada Estado miembro de la UE.

En el caso de Argentina, la Dirección Nacional de Protección de Datos Personales es un órgano dependiente de la Subsecretaría de Asuntos Registrales del Ministerio de Justicia, por tanto es dependiente del Poder Ejecutivo y, en consecuencia, tanto la designación como la remoción de su Director quedan supeditadas a la discrecionalidad del Presidente. Por ello y a pesar de tener entre sus facultades la de controlar el tratamiento de las bases de datos por parte del Estado, la misma queda comprometida por la condición de dependencia antedicha. El decreto reglamentario estableció como requisito para la selección del director el contar con "antecedentes en la materia", sin establecer mayores precisiones y quedando, por lo tanto, a discrecionalidad del Poder Ejecutivo la determinación y ponderación de tales antecedentes. Si bien el decreto reglamentario establece que la Dirección mantendrá su independencia, la misma carece de control financiero. La Dirección

tiene facultades de investigación, sanción, consulta, además de tener a su cargo el registro de las bases, tanto para el sector público como para el sector privado.

En el caso de la normativa chilena, la ley de protección de datos no hace referencia explícita en su articulado a una institución que vele por el cumplimiento de la norma. De tal suerte, los particulares se han visto desprovistos de una autoridad que fiscalice el cumplimiento de las disposiciones de la ley. La falta de institucionalidad solo posibilita a los titulares de los datos recurrir a la justicia en caso de verse afectados por un tratamiento no autorizado de sus datos. Cabe destacar que para el sector público se ha dado la siguiente situación: la ley 20.285 sobre Acceso a la Información Pública creó el Consejo para la Transparencia, que entre sus funciones principales tiene la de velar por el cumplimiento de la ley de Acceso a la Información; sin embargo también se le encomendó "velar por el adecuado cumplimiento de la ley 19.628 de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" (art. 33). Esto ha generado una situación dual, que por un lado ha llevado a determinados expertos a afirmar que la ley delegó el contralor de la protección de datos de las bases de datos públicos en el Consejo para la Transparencia pero con gran duda en cuanto al alcance de sus facultades[35]; mientras que otros autores indican que la injerencia del Consejo para la Transparencia en materia de tratamiento de datos personales es indirecta, pues solo proporciona directrices en orden a limitar la intervención estatal -cuando es un órgano de la administración del Estado el que realiza el tratamiento de datos personales- o cuando debe resolver reclamaciones en solicitudes de acceso a información pública que contenga datos personales, conforme a la normativa legal, sin tomar un rol activo en la defensa y promoción del resguardo de los mismos.[36]

El caso de México es más claro en cuanto al cumplimiento de requisitos por parte de la Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que es el órgano autónomo e independiente que tiene a cargo la aplicación y control de la normativa de datos, tanto respecto del sector público como del sector privado y que cuenta además con amplias facultades de investigación, de sanción, de consulta, etc.; encontrándose de tal suerte fuertemente alineado con lo que establece el RGPD.

En el caso de Brasil, dado la falta de una ley integral de protección de datos personales, sólo se puede indagar en lo que disponen las leyes sectoriales, y así cabe reiterar lo manifestado en el apartado 5.2.2.i.-, cuando se hizo referencia a que el Código de Defensa del Consumidor contiene previsiones relativas a la protección de datos aplicables a las bases de datos de consumidores, por lo que a tales efectos y en el ámbito específico de su incumbencia, puede inferirse que la Dirección Nacional de Consumidor dependiente del Ministerio de Justicia hace las veces de órgano de aplicación.

[35] Ver punto 3.1.2. del Reporte de Chile mencionado en el apartado 5.2.2. del presente trabajo.

[36] Ver Álvarez Valenzuela, Daniel. "Acceso a la información pública y protección de datos personales: ¿Puede el Consejo para la Transparencia ser la autoridad de contralor para la protección de Datos". Revista del Derecho, Universidad Católica del Norte. Vol. 23 Nº 1 Coquimbo, junio 2016. Accesible en http://bit.ly/2kRBUX5

ii.8.2 Sanciones La normativa europea prevé dos tipos de sanciones, la económica y la correctiva. Las multas económicas deben imponerse de manera individual efectiva, proporcionada y disuasoria y el monto de la sanción deberá ajustarse de acuerdo a las circunstancias del caso concreto. Entre los elementos a tener en cuenta figuran: la naturaleza, gravedad y duración de la infracción, la intencionalidad o negligencia en la infracción, las medidas tomadas para paliar la situación, etc. Las cuantías de las multas varían de acuerdo a la gravedad de la infracción y van desde un monto fijo (de hasta 10.000.000 o 20.000.000 de euros según la infracción) hasta un porcentaje -si se trata de una empresa- del 4% del negocio total anual global del ejercicio financiero anterior. Las procedencia y sanciones criminales serán decididas por casa Estado miembro de la UE.

En forma paralela, el RGPD dispone que la autoridad de control de cada país podrá imponer medidas correctivas en forma conjunta o en reemplazo de la multa. Estas medidas pueden consistir en advertencias, apercibimientos, órdenes de limitación, rectificación o supresión, retiro de la certificación, etc.

Las legislaciones de Argentina y México son las únicas que contienen disposiciones en tal sentido, en tanto establecen sanciones económicas y correctivas. Además incluyen la consagración de figuras penales para el caso de incumplimiento.

ii.8.3 Acciones y recursos El RGPD otorga al interesado (titutar) el derecho de presentarse ante la autoridad de aplicación si considera que el tratamiento de datos que le concierne infringe el Reglamento. Y también de recurrir por ante los tribunales para solicitar tutela judicial efectiva en caso de que los derechos que le otorga el RGPD hayan sido vulnerados como consecuencia de un tratamiento de sus datos personales. El tipo de procedimiento dependerá de la legislación procedimental de cada Estado miembro de la UE.

La legislación argentina da al titular del dato la posibilidad de presentarse ante la autoridad de aplicación para denunciar incumplimientos en el tratamiento de sus datos personales. También la ley contiene previsiones relativas al procedimiento judicial de habeas data, que dio contenido a y profundizó la consagración constitucional de esta figura. La normativa argentina dispuso que el habeas data se rija por las reglas del amparo y, en forma supletoria, por las del juicio sumarísimo.

En el caso de Chile, al no contar con una autoridad de aplicación, no existe posibilidad de que el titular de los datos recurra para denunciar incumplimiento. La legislación sólo contempla la acción de habeas data judicial, que deberá se interpuesta ante los tribunales ordinarios de justicia. México prevé una sistema que permite al titular efectuar reclamos ante el órgano de aplicación por incumplimiento de la normativa de protección de datos, que a estos efectos cuenta con facultades cuasi jurisdiccionales. Así estipula diversos procedimientos y recursos, incluyendo la conciliación entre el titular y el responsable. De tal suerte, será el órgano de contralor el que resolverá las divergencias entre el titular y el responsable del tratamiento. La posibilidad de recurrir a sede judicial será sólo

para desafiar la solución del órgano de aplicación. Debido a ello, la normativa mexicana no cuenta con un procedimiento de habeas data judicial.

ii.8.4 Compensación (daños y perjuicios) El RGPD establece expresamente el derecho de todo interesado a solicitar una indemnización por los daños y perjuicios materiales e inmateriales que hubiese sufrido como consecuencia de una infracción por parte del responsable o el encargado.

No existe una disposición similar en la ley argentina, en la cual la acción de habeas data permite al afectado tomar conocimiento de los datos personales almacenados o exigir su rectificación, supresión, confidencialidad o actualización pero no se prevé un resarcimiento por los daños sufridos. Si bien la ley 25.326 menciona en su art. 31 que los responsables de bases de datos están sujetos a la responsabilidad por daños y perjuicios derivados de la inobservancia de sus disposiciones, no está consagrado en forma expresa el derecho de los titulares a solicitar una indemnización, por lo que para cualquier reclamo el titular debería remitirse a las reglas generales del derecho civil.

La normativa chilena establece que el responsable de tratamiento deberá indemnizar los daños y perjuicios. Vale la pena aquí reproducir lo que destacan los colegas chilenos en su reporte: *"Además de lo comentado sobre los desincentivos que existen para accionar ante los tribunales ordinarios, el artículo 23 igualmente añade otros cuestionamientos. El primer inciso considera que para perseguir la responsabilidad del responsable del banco de datos en caso de un tratamiento indebido de los mismos, el actor debe probar el daño patrimonial y moral que sufrió como consecuencia de dicho tratamiento. En la práctica, es difícil saber quién tiene los datos del titular y qué hace con ellos, como ya vimos, el solo hecho de ejercer los derechos ARCO en el contexto chileno ya es bastante complejo. Dada esta situación, es poco probable que un titular sepa realmente dónde están sus datos y qué se está haciendo con ellos, considerando además la carencia de una autoridad de control que vele por el cumplimiento de la normativa. Por ello, es posible que solo pueda enterarse del daño producido por un tratamiento indebido con una amplia diferencia temporal de la autorización judicial."*[37]

La normativa mexicana de protección de datos no contiene previsiones específicas relativas a la compensación de daños y perjuicios, sino remisiones generales a la ley civil.

[37] Ver Reporte de Chile mencionado en el apartado 5.5.2. página 9.

Herramientas de enforcement, contenidas en la legislación de datos personales	Argentina	Chile	México	Brasil
Autoridad de aplicación y contralor				
De dedicación exclusiva	+	−	+	−
Independencia funcional	−	−	+	−
Presupuesto anual público e independiente	−	−	+	−
Con facultades de investigación y sanción	+	−	+	−
Sanciones				
Económicas	+	−	+	−
Correctivas	+	−	+	−
Penales	+	−	+	−
Acciones en cabeza del titular por incumplimiento LPD				
Acción ante la autoridad de aplicación	+	−	+	−
Acción judicial (hábeas data)	+	+	−	−
Compensación (reclamo judicial por daños y perjuicios)	−	+	−	−

Tabla 5.6.- Comparativa de Herramientas de Enforcement.[38]

VI Conclusiones y recomendaciones

Los datos personales tienen en el contexto actual un rol trascendental, provocado por los profundos cambios acontecidos en el entorno tecnológico y las transformaciones que lo anterior ha ocasionado en las prácticas de las empresas y en sus modelos de negocio, en los cambios organizacionales del Estado y en la modificación de la conducta en línea de los propios individuos. El aumento sustancial en los flujos transfronterizos motivado en la mayor integración económica y social y el mayor intercambio entre operadores públicos y privados, con más el notorio incremento de la economía digital ha generado un escenario en el que todos estos factores interactúan a tal punto que a veces se torna dificultoso establecer los límites entre ellos.

Cada vez más datos de los personas son recolectados, almacenados y son objeto de tratamiento de todo tipo, generando incluso nuevos datos a partir de ese tratamiento de los que el individuo en el que se originó la información ni siquiera está al tanto. No se trata solo de datos o contenido que el sujeto genera de manera consciente, sino también de aquellos datos que genera con cada movimiento que realiza en línea (*metadata*) y que por lo general desconoce y está más allá de su control.

Y es en este contexto complejo y de cambio vertiginoso en el que confluye el derecho al desarrollo económico y tecnológico de los pueblos, la libre iniciativa, y la libertad de competencia, pero también el derecho a la libertad de expresión, de comunicación y de opinión; el derecho a la inviolabilidad de la intimidad, de la vida privada, del honor y de la imagen; el derecho de acceso a la información; el derecho la privacidad y de la autodeterminación informativa.

[38] Tabla comparativa de elaboración propia.

A esto debemos agregar el fenómeno del *big data* (como denominación genérica de todo lo que refiere a enormes cantidades de datos y su tratamiento) y la toma de decisiones automatizadas mediante el uso de algoritmos, que según cierta doctrina y con la finalidad de mitigar los efectos de "la caja negra" (en referencia a los algoritmos a los que no se tiene acceso sea por cuestiones de propiedad intelectual o propiedad privada, sea porque escapan al entendimiento de la mayor parte de la población) han generado el derecho a la transparencia, el derecho a recibir explicación en los criterios en los que se basa la decisión, todo ello en concurrencia con el derecho a la no discriminación.

Los datos personales y la información que de su utilización y tratamiento puede generarse, pone al individuo en el centro de la escena. Las herramientas para el ejercicio del derecho a la autodeterminación informativa que las legislaciones de protección de datos de la década de 1990 contienen pueden parecer insuficientes ante nuevas realidades. La decisión algorítmica, el aprendizaje automático (*machine learning*) o la inteligencia artificial, dejan poco lugar para el consentimiento o el control que el individuo pueda dar o hacer respecto de su información.

Es así como diversas instancias internacionales han comenzado a elaborar lineamientos y principios tendientes a fortalecer la protección de la privacidad y de los datos personales, a la vez que buscan resguardar y equilibrar los demás derechos que confluyen en este esquema. El Reglamento General de Protección de Datos de Europa es el ejemplo más acabado de lo antedicho.

A la luz de estas circunstancias, inquietudes y nuevas dinámicas, toca mirar a América Latina. El análisis de las características de los sistemas de protección de datos de cuatro países, Argentina, Chile, Brasil y México nos permite afirmar que en general todos ellos cuentan con previsiones constitucionales sólidas relativas al reconocimiento y protección de la privacidad y la autodeterminación informativa como figuras jurídicas diferenciadas. También cuentan en general con previsiones normativas específicas, aunque con debilidades estructurales en el caso de Chile y con la significativa excepción de Brasil, que no tiene una ley comprensiva de protección de datos personales.

Los principios rectores del tratamiento de datos personales también resultan coherentes con los reconocidos internacionalmente, aunque no contienen referencia al principio de minimización ni de responsabilidad proactiva.

El consentimiento tiene un papel fundamental en los sistemas de los países analizados, sin que el "interés legítimo" del responsable sea suficiente por sí mismo para el tratamiento de los datos, tal y como lo es en el sistema europeo.

Los derechos reconocidos por estos sistemas nacionales a los titulares de los datos son consistentes con la tradicional línea protectoria, de acceso, rectificación, cancelación y oposición. E incluso algunas de las legislaciones contienen previsiones relativas a herramientas más novedosas, tales como el derecho a la portabilidad y el derecho a un tratamiento leal y transparente para el caso de decisiones automatizadas.

La normativa europea trae dos novedades en este sentido, el derecho a la limitación del tratamiento y el derecho a la supresión o derecho al olvido, tal el nombre con el que erróneamente ha trascendido. Este último derecho que reconoce el Reglamento europeo está más bien vinculado a lo que desde ADC preferimos denominar el "derecho a ser desindexado". Este derecho ha suscitado acaloradas discusiones en numerosos foros, entre aquellos que sostienen que su adaptación generaría una vulneración al derecho de libertad de expresión y aquellos que sostienen que es parte esencial del derecho de autodeterminación informativa. El tenor de este trabajo no permite ahondar en la consideración y análisis de estas tensiones, que están siendo objeto particular de estudio.

En consonancia con las medidas de protección que la normativa europea pone en cabeza de los responsables de tratamiento, sólo se puede mencionar a la legislación mexicana. Las previsiones relativas a la privacidad por defecto y por diseño, la notificación en caso de violaciones de seguridad al interesado y/o a la autoridad de aplicación, la figura del delegado de protección de datos o la evaluación de impacto o riesgo se encuentran mayormente ausente de los sistemas latinoamericanos analizados.

Los requisitos para la cesión y para la transferencia internacional de datos son prácticamente nulos, con excepción de la normativa argentina.

Por último, cabe destacar que las herramientas de enforcement, es decir, aquellas que permiten la aplicación efectiva de las garantías, derechos y protecciones que consagran la normativa, con excepción de México, son en general deficitarias. En el caso de Argentina, las debilidades señaladas del órgano de contralor resultan incompatibles con el real ejercicio de los derechos y garantías que la misma ley establece. En el caso de México, la ausencia de la acción de habeas data ha sido referida como una debilidad, a pesar de las múltiples acciones previstas en el proceso administrativo y las facultades del órgano de aplicación. La situación es más grave en el caso de Chile y Brasil, donde la ausencia de herramientas efectivas de enforcement es total.

Así, el estudio de estos cuatro países muestra que a pesar de contar con un soporte constitucional que aparece como robusto, en la práctica generan un escenario que se caracteriza por su disparidad y fragmentación, con debilidades estructurales y una relativa –más bien negativa– capacidad de enforcement.

De tal suerte, el estudio de los sistemas de Argentina, Chile, Brasil y México, sugiere la necesidad de:

Fortalecer los estándares de protección de los datos personales y sus mecanismos de enforcement. Dado el contexto descripto, la ponderación y adopción de nuevas previsiones aparecen como necesarias en pos del fortalecimiento de los estándares hoy por hoy vigentes. Figuras como la de los principios de minimización y responsabilidad proactiva o el derecho a la portabilidad, como así también el mayor detalle y análisis de viabilidad de medidas concretas en

cabeza de los responsables que aseguren el mejor tratamiento posible de los datos personales se presentan como de discusión necesaria. La generación de vías más efectivas de información para el individuo, que sea clara, concisa y pertinente y le posibilite la comprensión acabada de la suerte de sus datos personales es todavía materia pendiente.

Especial atención merecen los mecanismos y herramientas que posibiliten la efectiva implementación, aplicación y control de las protecciones y garantías (enforcement), que han aparecido como una de las principales deficiencias y obstáculos para el desarrollo de los sistemas de protección de datos personales.

Generar mecanismos dinámicos y multiparticipativos que permitan identificar y contener los riesgos generados por los avances tecnológicos. El desarrollo de fenómenos como el big data, el internet de las cosas, la decisión algorítmica, el aprendizaje automático o la inteligencia artificial ponen en jaque elementos fundantes del sistema de protección de datos, tal como la noción de consentimiento. De tal suerte, surgen figuras como la del « interés legítimo » o la del « uso compatible de datos» que habilitan facultades de tratamiento más allá del conocimiento y consentimiento de su titular. La adopción de decisiones automatizadas y la elaboración de perfiles mediante algoritmos que pocos conocen o entienden excluyen, paradójicamente, a su protagonista principal. La generación de canales y mecanismos dinámicos y con participación de referentes de los diversos sectores involucrados (funcionarios de protección de datos, sector privado y técnico, academia y sociedad civil) aparece como necesaria para la adecuada identificación, comprensión, contención y conciliación de estas circunstancias, y la consecuente generación de alternativas coherentes con el derecho de autodeterminación informativa.

Propiciar instancias de interacción y diálogo para el fortalecimiento de la autedeterminación informativa y su confluencia con otros derechos humanos. La contundencia del derecho a la autodeterminación informativa, en tanto garantiza al individuo el control de sus datos, genera innumerables y permanentes situaciones de conflicto con otros derechos, también esenciales para su adecuado desarrollo. Más allá de las vías procedimentales y judiciales, en las que en última instancia transcurrirán y se resolverán los conflictos en cuestión, la generación de espacios de interacción y diálogo que posibiliten el debate riguroso, experto y permanente de las diversas situaciones de confluencia de los derechos en cuestión posibilitará la generación de expertise e insumos que redunden en un fortalecimiento del ejercicio del derecho a la autodeterminación informativa como parte integrante del conjunto de derechos humanos del individuo.

Propender a la armonización legislativa. Los vertiginosos avances tecnológicos generan desafíos que trascienden límites geográficos. El incremento en el flujo transfronterizo de datos pone de

manifiesto la necesidad de incluir a la armonización legislativa como un aspecto de revelancia no sólo para el fortalecimiento de los propios sistemas de protección de datos, sino también con miras en el desarrollo de la economía digital de los países en cuestión y de la región.

Prestar especial atención a situaciones particulares. Si bien, como ya se dijo en el apartado dedicado a la metodología, este trabajo se focalizó en aspectos generales de los sistemas de protección de datos, se pone de resalto que las recomendaciones anteriores también deberán considerarse, previo estudio, en relación a supuestos especiales de tratamiento de datos, tales como los datos sensibles, los datos financieros, los datos de salud, los datos en poder de autoridades policiales y de seguridad, por nombras algunos. Como así también en el caso del tratamiento de datos que realiza el Estado, en tanto goza de excepciones elevadas.

Cabe agregar que la Red Iberoamericana de Protección de Datos Personales aparece como una de las posibles instancias de diálogo e interacción, ya que además de la significativa representación de autoridades de protección de datos y de privacidad de países de la región y de organismos internacionales, ha previsto en sus reuniones la participación del sector privado y de observadores académicos y, en forma muy reciente, ha admitido la participación de un representante de sociedad civil. Claro está que sería deseable que los mecanismos de participación fueran más abiertos.

Sin perjuicio de ello, el proceso de revisión y reforma legislativa de los países seleccionados se presenta como una oportunidad para reflexionar acerca de las diversas cuestiones que aquí se desarrollaron y, en su caso, adoptar las medidas conducentes.

Por último, resta decir que las reflexiones, conclusiones y recomendaciones contenidas en este documento no buscan ser posiciones acabadas y definitivas, sino que por el contrario tienen como objetivo ser disparadores de necesarios diágolos, debates e interacciones que se presentan como ineludibles para el fortalecimiento de derechos humanos no sólo en Argentina, Chile, Brasil y México, sino en toda Latinoamérica.

por los Derechos Civiles