EL RGPD Y LA LEY ARGENTINA DE PROTECCIÓN DE DATOS PERSONALES

Análisis comparativo

por los Derechos Civiles

Introducción:[1]

El 27 de Abril de 2016 el Parlamento Europeo y el Consejo de la Unión Europea (UE) sancionaron el Reglamento General de Protección de Datos (RGPD)[2] que sustituye a la vieja Directiva 95/46, instrumento normativo que reguló la protección de datos personales en la UE por más de veinte años. La principal característica general de este Reglamento es que, a diferencia de la Directiva -que necesitaba de la transposición por las leyes nacionales de los países miembros para su entrada en vigencia-, su aplicación es inmediata ya que no hay necesidad de incorporación por parte del ordenamiento jurídico interno. Por el contrario, el Reglamento desplazará cualquier norma interna en las materias que regule. Como excepción, únicamente cuando el propio Reglamento lo disponga expresamente, las legislaciones nacionales podrán dictar regulación complementaria. Finalmente, la nueva normativa entró vigor el 25 de Mayo de 2018, ya que se previó un plazo de dos años -a contar desde el 25 de mayo de 2016- para el inicio de su aplicación, en virtud de que se consideró prudente otorgar a los sujetos afectados por la nueva regulación un tiempo razonable para poder adaptarse a las flamantes exigencias legales. El RGPD consiste en 99 artículos reunidos en 11 capítulos y cuenta con 173 considerandos que sirven como explicación de las disposiciones y eventualmente pueden servir como pautas para su interpretación.

A causa de su reciente sanción, el Reglamento es un instrumento normativo actualizado, por lo que el fenómeno de las nuevas tecnologías de la información y la comunicación (TIC) ha sido considerado, sobre todo en lo que se refiere a las amenazas y potenciales afectaciones que puedan ocasionar a la protección de los datos personales. En paralelo a esto, debemos recordar que la legislación argentina se ha inspirado en gran medida en el modelo europeo de protección de datos. Como ejemplo, podemos mencionar que nuestra ley de protección de datos personales se basa en la ley española de 1992 (reemplazada en 1999 por la actual Ley Orgánica de Protección de Datos de Carácter Personal). Debido a estas consideraciones, no resulta ocioso realizar un análisis comparativo de nuestra legislación con el RGPD, a fin de ver cuáles son las diferencias de regulación y detectar aquellas áreas que nuestra legislación no ha regulado en virtud de que el momento

[1] El presente informe fue elaborado por Eduardo Ferreyra, Abogado y Analista de Políticas Públicas del Área Digital de la Asociación por los Derechos Civiles.
[2] Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

de su sanción no permitía prever las características de la expansión del fenómeno digital en los siguientes años. Es por ello que a continuación, describiremos las principales novedades que el Reglamento ha traído y lo compararemos con lo dispuesto en la legislación argentina.

Objeto (art. 1): El RGPD dispone que su objetivo es establecer normas que se refieran tanto a la protección de los datos personales de las personas físicas como a la libre circulación de aquellos datos. Debido a esta doble función, si bien la normativa establece la protección de los derechos y libertades fundamentales de las personas físicas -en particular el derecho a la protección de datos personales en sí mismo-, también sostiene que este fin no puede restringir ni prohibir la libre circulación de datos dentro del mercado interior de la UE.

La ley 25326 también establece como objetivo la protección integral de los datos personales aunque los considera como un medio para proteger el derecho al honor y a la intimidad de las personas, así como el acceso a la información. Por otra parte, no solamente las personas físicas están cubiertas por la legislación sino que las personas jurídicas también podrán ampararse en la normativa "en cuanto resulte pertinente", según el lenguaje de la ley.

Finalmente, ésta última contiene una referencia a que no se podrán afectar las bases de datos ni las fuentes de información periodística. En este sentido, el RGDP dispone que los tratamientos de datos personales con fines periodísticos deben gozar de excepciones a ciertas disposiciones del Reglamento pero deja a cada Estado miembro la determinación de cuáles serán esas exenciones.

Ámbito de aplicación material (art. 2): El criterio establecido por el Reglamento para su aplicación es la actividad desarrollada, a saber, la realización de un proceso de tratamiento -automatizado o no- de datos personales contenidos o destinados a estar en un fichero. En cambio, en la ley argentina el criterio es el lugar en donde están contenidos los datos personales, en este caso, que se encuentren en una base de datos pública o privada destinada a dar informes.

Por otro lado, el Reglamento establece que sus disposiciones no se aplicarán al

tratamiento de datos personales realizados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales. Esto es así debido a que en forma conjunta se sancionó la Directiva 2016/680, que establece un marco autónomo y detallado para regular este tipo de tratamiento de datos. Por el contrario, en la ley argentina existen disposiciones que regulan las bases de datos de las fuerzas de seguridad y/o policiales, aunque en forma escueta.

Ámbito de aplicación territorial (art.3): El Reglamento establece dos supuestos para su aplicación territorial: el primero se produce cuando el tratamiento de datos se realiza en el contexto de actividades de un establecimiento situado en la UE, con independencia de que el tratamiento tenga lugar o no en la UE. El segundo supuesto aparece cuando hay tratamiento de datos personales de interesados que viven en la UE por parte de un responsable o encargado que no reside en la UE, siempre que la actividad de tratamiento de datos se vincule con la oferta de bienes y servicios a dichos interesados o con el control de su comportamiento, en la medida que tenga lugar en la UE.

En la ley argentina, sólo se habla de "archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes" sin mencionar la sede de su establecimiento ni el lugar en el que se lleva a cabo el tratamiento de datos como criterio para su aplicación territorial. La única referencia en este sentido está dada por el art. 44, que somete a la jurisdicción federal a los "registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional".

Definiciones (art. 4): El Reglamento contiene un amplio catálogo de definiciones acerca de conceptos que son considerados decisivos para la regulación del tratamiento de datos personales. En este sentido, la lista es mucho más larga que la prevista por la ley argentina. Entre los conceptos incorporados por el Reglamento y que no figuran en la ley 23.526 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, entre otros.

Por otra parte, la definición de datos personales del Reglamento 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". Por el contrario, la ley argentina no cuenta con ningún criterio o definición para establecer el carácter identificable de una persona.

Respecto a los datos sensibles, el Reglamento -que las denomina "categorías especiales de tratamiento de datos"- incluye varios datos ya previstos por la ley argentina, 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 que no están previstos en la legislación argentina, como los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física y los datos relativos a la orientación sexual de una persona. A su vez, la ley 25326 considera como dato sensible a los datos que revelen convicciones morales, situación no prevista por el Reglamento.

En relación a los sujetos contemplados, la ley argentina reconoce tres supuestos: el titular de los datos (aquel cuyos datos son objeto de tratamiento), el responsable de la base de datos (quien es titular de un archivo de datos) y el usuario de los datos (quien realiza el tratamiento de datos). Por el lado del Reglamento, existe un número más amplio de sujetos definidos por la ley: el interesado (término con que se denomina en la normativa europeo a lo que en la ley argentina se conoce como titular de los datos), el responsable (similar al previsto en la normativa argentina), el encargado (aquel que trate datos personales por cuenta del responsable del tratamiento), el destinatario (aquel al que se comuniquen datos personales, se trate o no de un tercero), el tercero (aquella persona distinta del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado) el representante (quien representa al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del Reglamento). Asimismo, se contemplan definiciones de empresa, grupo empresarial, organización internacional autoridad de control y autoridad de control interesada.

Por último, se contempla a los servicios de la sociedad de la información, para cuya definición se remite a los afirmado por la Directiva (UE) 2015/1535 , que establece que es

"todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios"[3]

Principios (art. 5): En principio, existe una relativa similitud entre los principios consagrados en ambas legislaciones. Así, los dos ordenamientos reconocen los principios de licitud, 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 y observa los principios establecidos en la ley, el Reglamento (art. 6) establece una serie detallada y precisa de condiciones las cuales -al menos una- deben ser cumplidas para ser considerado lícito el tratamiento, a saber: si el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; si el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; si el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; si el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o si el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Asimismo, mientras la ley argentina define al principio de finalidad como aquel mediante el cual los datos no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención, el Reglamento consagra que los datos pueden ser "recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines".

[3] Directiva (UE) 2015/1535 por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32015L1535&from=ES

Por otro lado, el Reglamento consagra explícitamente el principio de minimización de los datos, que ordena que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". De esta manera, la normativa europea dispone como principio general la obligación de recolectar, almacenar y procesar la menor cantidad de información posible.

La limitación de la conservación también está definida de manera precisa por el Reglamento, que establece que los datos sean "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"

En sintonía, la normativa europea consagra el principio de integridad y confidencialidad, ordenando que los datos sean "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 ".

Finalmente, el Reglamento agrega el principio de responsabilidad proactiva, por el cual los responsables de tratamiento de datos serán responsables del cumplimiento de todos los principios y además, deberán ser capaces de demostrar tal cumplimiento.

Consentimiento (art. 7): En el Reglamento el consentimiento constituye una de las bases legítimas por las 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 la UE sino que coexiste con otras bases legítimas establecidas 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.

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 la legislación argentina y admite además de una declaración, la presencia de otras "acciones afirmativas claras" que sean expresión del consentimiento del interesado. En este último sentido, la ley argentina determina que el consentimiento sólo puede otorgado por escrito o por otro medio que se le equipare.

Otra diferencia con la normativa argentina es que el Reglamento establece expresamente que es el responsable del tratamiento de datos el encargado de demostrar que el interesado consintió en que sus datos personales sean tratados. Asimismo, la normativa europea determina que para establecer el carácter libre del consentimiento, deberá tenerse en cuenta los datos personales que se solicitan para la ejecución del contrato. Si la persona debe suministrar o aceptar el tratamiento de datos que no son necesarios para la ejecución de dicho contrato, tal situación será tomada como un elemento en contra de considerar al consentimiento como libre.

Finalmente, el Reglamento contiene disposiciones referidas al consentimiento prestado por menores de edad en relación a los servicios que se le ofrecen (art.8). La norma ordena que el consentimiento será considerado lícito cuando el menor tenga como mínimo dieciséis (16) años. Si es menor de esa edad, el consentimiento debe ser dado por el o la titular de la patria potestad o por el que ejerza la tutela. Por el contrario, en la legislación argentina no hay disposiciones referentes al consentimiento de menores de edad.

Datos sensibles (art. 9): Además de las diferencias en cuanto a qué se considera

dato sensible (vistas más arriba) existen divergencias en la forma de regular su tratamiento. Según el Reglamento, la regla general es la prohibición de todo tratamiento referente a este tipo de datos. Sin embargo, existen una serie de situaciones en las cuales el tratamiento de datos sensibles estaría autorizado. La primera contemplada es el consentimiento explícito del interesado. Luego, el Reglamento despliega un listado de excepciones que funcionan como permisos para tratar datos sensibles (entre ellas, la necesidad de cumplir con derechos y obligaciones del responsable, la existencia de un interés vital del interesado o de otra persona física, la presencia de un interés público esencial, etc). En definitiva, lo importante es la existencia de una base legal que justifique el tratamiento de datos sensibles.

En forma similar, la ley argentina establece la prohibición de formar bases de datos que revelen datos sensibles. Asimismo, también dictamina que ninguna persona puede ser obligada a proporcionar datos sensibles. Sin embargo, al momento de establecer las excepciones, la ley sólo se refiere a la existencia de "razones de interés general autorizadas por ley" y no contiene un listado detallado de salvedades, al estilo del Reglamento.

Finalmente, ambas legislaciones disponen que los registros de antecedentes penales deben quedar siempre bajo control de las autoridades públicas.

Derechos de los interesados o titulares de los datos (arts. 13 a 21): Al igual que la ley argentina, el Reglamento 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 tres nuevos derechos no previstos -o previstos de manera distinta-en la ley 25326.

El primero es el 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.

El segundo derecho incorporado es el 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.

El tercer derecho que se agrega es el 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.

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 el caso de estas bases de daos. 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.

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.

La doctrina[4] 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.

Esta disposición podrá ceder en los siguientes casos: cuando sea necesario para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; esté autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y asimismo establezca medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o cuando haya un consentimiento expreso del interesado.

Tal como lo vimos al momento de describir la legislación vigente, la ley argentina declara que las decisiones que se basen únicamente en un tratamiento informatizado de datos personales serán consideradas insanablemente nulas. Sin embargo, esta disposición

[4] 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

únicamente se aplica a decisiones judiciales o administrativas, con los que quedan fuera de su regulación las entidades privadas, que son las que actualmente hacen un uso intensivo de las tecnologías de Big Data para la toma de decisiones automatizadas.

Medidas técnicas y de seguridad: Tanto el Reglamento como la ley 25.326 coinciden en establecer la obligación para los responsables de bases de datos de implementar medidas técnicas y organizativas que garanticen el cumplimiento con las disposiciones de las normativas respectivas. Sin embargo, el Reglamento establece numerosas disposiciones que detallan algunas de las medidas o herramientas que los responsables deben implementar para asegurar la licitud de sus tratamientos de datos, cuestión que está ausente en la ley 23.326.

Entre los tipos de medidas a adoptar se encuentran:

- Registro de las actividades del tratamiento (art. 30): A diferencia de Argentina, los responsables de tratamiento de datos no deben inscribir sus bases de datos en ningún registro pero sí tienen la obligación de llevar un registro de las actividades de tratamiento de datos que realizan, las cuales deben estar a disposición de las autoridades de control cuando éstas lo requieran. Esta obligación no se aplica a aquellas empresas u organizaciones que empleen menos de 250 personas, a menos que el tratamiento pueda entrañar un riesgo para los derechos o libertades fundamentales de los interesados, incluya datos sensibles o se refiera a datos sobre condenas penales.

- Privacidad por diseño y por defecto (art. 25): La primera consiste en la obligación de todo responsable de tratamiento de aplicar desde el mismo momento en que se determina los medios de tratamiento todas las medidas necesarias (seudominización, limitación del tratamiento, etc) para respetar la privacidad de los usuarios. 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 encuentra el deber de garantizar por defecto que todo tratamiento de datos tenga como objeto sólo aquellos necesarios para los fines de su actividad. Asimismo, estas medidas deben garantizar que los datos personales no sean

accesibles a un número indeterminado de personas.

- Medidas de seguridad adecuadas (art. 24): El Reglamento establece que los responsables o encargados de tratamiento de datos deben adoptar medidas adecuadas para garantizar un nivel de seguridad adecuado al riesgo que dicho tratamiento puede implicar para los derechos y la libertades de las personas. Para evaluar dicho riesgo, se deberán tomar en cuenta los riesgos que pueda presentar la eventual destrucción o alteración de la base de datos o el acceso no autorizado a dichos datos. Además del riesgo, las medidas a adoptar deben tener en cuenta el estado de la técnica, los costos de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento. Asimismo, se establece la obligación de incluir en el registro de actividades la descripción de las medidas de seguridad adoptadas, en cuanto sea posible. Por último, se considera que la adhesión a un código de conducta o a un mecanismo de certificación constituye un elemento para demostrar el cumplimiento de los requisitos de seguridad.

- Notificación de una violación de seguridad (art. 33 y 34): En caso de una violación a la seguridad de los datos personales, el Reglamento dispone que el responsable debe notificar de inmediato -o a más tardar en 72 horas- a la autoridad de control. En caso de que se lo haga después del plazo, se deberá indicar los motivos de la demora. La excepción a la notificación tendrá lugar cuando sea improbable que la violación constituya un riesgo para los derechos y las libertades de las personas físicas. Por otro lado, el responsable tendrá la obligación de documentar todos los incidentes ocurridos, sus causas y las medidas correctivas adoptadas. Respecto al titular de los datos o interesado, el Reglamento establece la obligación por parte del responsable o encargado de comunicarle sin dilación indebida la violación únicamente cuando exista un alto riesgo para los derechos y las libertades de las personas físicas. Este deber puede eximirse cuando: el responsable ya haya adoptado medidas de protección apropiadas -en particular aquellas que hagan ininteligibles los datos personales a personas no autorizadas a acceder a los mismos, como el cifrado-, el responsable ha tomado medidas ulteriores que garantizan que ya no existe el riesgo o cuando suponga un esfuerzo desproporcionado. La autoridad de control

puede decidir que existe un alto riesgo y así obligar a los responsables a notificar la violación a los interesados.

- Evaluación de impacto de protección de datos (art. 35 y 36): Cuando sea probable que un tratamiento de datos presente un alto riesgo para los derechos y libertades de las personas físicas, el Reglamento prevé la obligación por parte del responsable o encargado de realizar una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. En particular, evaluación se exigirá en caso de: 1. elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; 2. tratamiento a gran escala de las categorías especiales de datos ("datos sensibles" según la terminología de la ley argentina) o de datos relativos a condenas penales, y 3. observación sistemática a gran escala de una zona de acceso público. Asimismo, cada autoridad de control tiene la facultad de decidir qué operaciones necesitarán evaluación y cuáles no. Finalmente, el Reglamento prevé un contenido mínimo de la evaluación y determina que cuando proceda, se deberá recabar la opinión de los interesados. Cuando la evaluación demuestre que la operación de tratamiento implica un alto riesgo si no se adoptan medidas para mitigarlo, el responsable deberá consultar en forma previa a la autoridad de control antes de iniciar la actividad de tratamiento
- Delegado de protección de datos (arts. 37 a 39): El DPD es una figura creada por el Reglamento y constituye una de las principales novedades del futuro sistema europeo de protección de datos personales. El reglamento establece que los responsables y encargados del tratamiento deberán designar uno cuando: el tratamiento se realice por una autoridad u organismo público (con excepción de la función judicial), las actividades principales del responsable consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala; o cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de datos sensibles o datos relativos a condenas penales. El nombramiento del delegado se hará en base a sus cualidades personales, su conocimiento especializado del Derecho y la práctica en materia de protección de datos y la capacidad para

desempeñar sus funciones. Asimismo, su vinculación con el responsable o encargado podrá hacerse a través de su incorporación a la plantilla del personal o mediante un contrato de servicios. Para garantizar su independencia, el delegado no podrá recibir instrucciones del responsable ni podrá ser sancionado o destituido por el mismo. Por otro lado, podrá ser contactado en cualquier momento por los interesados para cualquier cuestión relativa la protección de sus datos. Sus funciones serán las de: informar y asesorar sobre las obligaciones impuestas por la normativa sobre protección de datos, supervisar el cumplimiento de dicha normativa (en particular, lo que respecta a la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorías correspondientes), ofrecer asesoramiento sobre la evaluación de impacto sobre protección de datos y cooperar o actuar de punto de contacto con la autoridad de control para cuestiones relativas al tratamiento de datos.

Transferencia internacional de datos (art. 44 a 49): Tanto el Reglamento 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 Reglamento 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 o por una autoridad de control, un código de conducta o mecanismo de certificación.

Si tampoco pueden ofrecerse garantías adecuadas, el Reglamento establece una última lista de supuestos en los cuales procede la transferencia, a saber: cuando el interesado 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 Reglamento, nuestra legislación consagra un corto catálogo de excepciones. La ley 25326 establece las siguientes (art.12): 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.

Órgano de control (arts. 51 a 54): El Reglamento establece que todas las autoridades de control de los países miembros deberán actuar con total independencia en el desempeño de sus funciones. Asimismo, los miembros serán ajenos a toda influencia externa y no solicitarán ni admitirán ninguna instrucción. Por otro lado, se dispone que todo Estado debe garantizar que su autoridad de control cuente en todo momento con los recursos humanos, técnicos y financieros, así como los locales y la infraestructura necesaria para el cumplimiento efectivo de sus funciones. Finalmente, la normativa ordena que todos los Estados garanticen que los órganos de control gocen de un presupuesto anual público e independiente y que estén sujetos a un control financiero que no afecte su independencia.

Estas disposiciones pueden ser contrastadas con lo dispuesto por la ley argentina y

sobre todo con lo que sucede en la práctica con nuestro órgano de control. Como se dijo anteriormente, si bien estaba previsto el carácter descentralizado y la autonomía funcional de la autoridad de controlar, finalmente cuestiones financieras hicieron que estas disposiciones fuesen vetadas por el Poder Ejecutivo de turno. Como resultado, la Dirección Nacional de Datos Personales (DNPDP) se transformó en un órgano dependiente del Poder Ejecutivo y que no contaba con los recursos financieros necesarios para cumplir con todas las funciones que le ordena ley de protección de datos personales.

En Septiembre de 2017 hubo un importante cambio organizativo. A través del Decreto de Necesidad y Urgencia 746/2017[5] el Poder Ejecutivo modificó las atribuciones de la recientemente creada Agencia de Acceso a la Información Pública (AAIP) para agregarle la función de autoridad de protección de datos. Así, la DNPDP fue absorbida por la AAIP, organismo que según su ley de creación, tiene carácter autárquico y posee autonomía funcional dentro del ámbito del Poder Ejecutivo. El titular de la AAIP durará en su cargo cinco años y es designado por el Poder Ejecutivo luego de un procedimiento de selección abierto, público y transparente. Dentro de la AAIP, existe una nueva Dirección de Protección de Datos Personales, cuyas funciones continúan siendo las mismas que fueron establecidas por la ley 25326

En lo que respecta a las funciones a desarrollar, la normativa europea cuenta con un catálogo más numeroso de tareas a ser desempeñadas por las autoridades de control, y por consiguiente, sus poderes de investigación son mucho más amplios que las de la autoridad de control argentina.

En efecto, de acuerdo a la ley 25326, la DNPDP posee funciones de asesoramiento a las personas que vean afectadas sus datos personales, de promulgación de normas y reglamentos necesarios para el cumplimiento de la ley, de control de los requisitos que las bases de datos deben cumplir para poder inscribirse en el registro y de requerimiento de información a entidades -públicas o privadas- relativas al tratamiento de datos que realizaren. Por otro lado, la DNPDP puede imponer sanciones administrativas en caso de

[5] Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/279940/norma.htm

violación a la ley y constituirse como querellante penal en caso de cometerse alguna infracción criminal prevista por la normativa.

Finalmente, el órgano de control puede controlar el cumplimiento de las medidas de seguridad adoptadas por las bases de datos. Para ello, incluso puede solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la ley.

En el caso del Reglamento – como dijimos anteriormente- las funciones son más numerosas. A manera ejemplificativa, podemos mencionar las siguientes: controlar la aplicación del Reglamento, promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento; tratar las reclamaciones presentadas e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable; llevar a cabo investigaciones sobre la aplicación del Reglamento; hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales, entre otras. Para llevar a cabo esta tarea, las autoridades disponen de amplios poderes de investigación y de corrección. Entre los primeros se cuentan: llevar a cabo auditorías de protección de datos, revisiones de las certificaciones, ordenar la facilitación de cualquier información necesaria para el desempeño de las funciones, obtener el acceso a los datos personales, los equipos y medios de tratamiento de datos. Entre los segundos podemos mencionar la facultad de imponer sanciones (advertencia, apercibimiento, multa o la limitación -temporal o definitiva- del tratamiento) ordenar la supresión, rectificación o limitación de un dato personal, ordenar a los responsables o encargados que sus operaciones se ajusten al Reglamento, que atiendan las solicitudes de los interesados en ejercicio de sus derechos o que notifiquen a dichos interesados en caso de un incidente de seguridad.

Responsabilidad e indemnización (art. 82) : El Reglamento 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. Por el contrario, 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.

Sanciones (art. 83): En la normativa europea se prevén dos tipos de sanciones. La primera y más importante es la multa económica. El Reglamento dispone que las mismas deben imponerse de manera individual efectiva, proporcionada y disuasoria. De esta manera, el monto de la sanción debe 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. En forma paralela, se dispone que las autoridades de control de cada país tendrán la capacidad de 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.

Respecto a las cuantías de las multas, las mismas 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.

En lo que respecta a Argentina, la ley ha otorgado al órgano de control un listado de sanciones que van desde el apercibimiento y la suspensión hasta la imposición de multas (de $1.000 a $100.000) y la cancelación de la base de datos. Asimismo, también se determina que las sanciones deben aplicarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción. Por último se establece que toda sanción debe imponerse garantizando el principio del debido proceso.

La principal diferencia que se observa entre ambas normativas es la cuantía de las sanciones económicas. Por un lado, el monto al que pueden alcanzar las sanciones en la UE es mucho más alto que en Argentina. Por otro lado, en el Reglamento existe la facultad de aplicar una multa mediante un porcentaje del negocio total, mientras que la ley 25.326 no ha consagrado esa prerrogativa. La ausencia de la posibilidad de imponer multas por porcentaje puede constituir un obstáculo para la capacidad de los órganos de control de hacer cumplir

la ley, ya que muchas veces los montos fijos son muy bajos o quedan desactualizados por la marcha de la economía. De esta manera, los responsables prefieren pagar la multa antes que cumplir con sus deberes, los cuales pueden resultar aún más onerosos que la sanción.

Bases de datos en manos de fuerzas de seguridad o policiales: El Reglamento no contiene disposiciones al respecto. Sin embargo, esto no se debe a un grosero descuido. En forma paralela, la Unión Europea sancionó la Directiva 680/2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. La mencionada norma entró en vigor el 5 mayo de 2016 **y** tiene como principal finalidad el garantizar la adecuada protección de los datos de las víctimas, testigos e investigados por la presunta comisión de delitos. Paralelamente la Directiva pretende armonizar la cooperación transfronteriza de la policía y los fiscales para combatir más eficazmente el crimen y el terrorismo en toda Europa.

La Directiva establece que los principios generales de protección de datos personales también deben aplicarse al tratamiento de este tipo de información. Asimismo, se introducen disposiciones especiales en razón de la particular naturaleza de los datos tratados. Así, se establece la necesidad de fijar plazos para la supresión de los datos personales almacenados o para una revisión periódica de la necesidad de conservar los mismos. También se dispone que los responsables del tratamiento deben distinguir claramente entre las distintas clases de interesados, como: personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal, personas condenadas por una infracción penal, víctimas de una infracción penal o terceras partes involucradas en una infracción penal. Otro principio que se consagra es la obligación de distinguir -en la medida de lo posible- los datos personales basados en hechos de aquellos datos personales basados en apreciaciones personales. Por último -sólo a los fines de esta breve descripción-, se establece la prohibición de aquellas decisiones que estén basadas únicamente en un tratamiento automatizado -incluida la elaboración de perfiles- que produzcan un efecto negativo en el interesado. Si bien esta prohibición puede ser dejada de lado por el derecho interno, en ese caso se debe procurar que se tomen medidas adecuadas para resguardar los derechos y libertades del interesado, al menos el derecho a obtener la intervención humana por parte del responsable del tratamiento.

En lo que atañe a la normativa argentina, las regulaciones sobre este tipo de tratamiento de datos son muy escasas. En la ley 25.326 encontramos un único artículo -el 23- que se ocupa de ofrecer algún tipo de guía normativa. Pero esta disposición presenta problemas debido a su indeterminación y amplitud. Asimismo, tampoco establece las obligaciones que la Directiva europea ha consagrado para el tratamiento de este tipo de datos. En conclusión, las bases de datos de las fuerzas de seguridad y/o policiales gozan de una importante discrecionalidad, ya que se encuentran pobremente reguladas por la normativa argentina. Como consecuencia, los ciudadanos encuentran numerosas dificultades para ejercer la principal herramienta de protección de sus datos.

Conclusión: La sanción del Reglamento General de Protección de Datos ha supuesto la mayor novedad de los últimos tiempos en materia de protección de datos personales. La influencia de sus principios y de sus normas seguramente se extenderá más allá de Europa. En ese sentido, Argentina seguramente será de las primeras en acusar su impacto. Hay dos razones principales para ello. La primera tiene que ver con que el sistema de protección de datos personales argentino está fuertemente inspirado en el modelo europeo. Como resultado, no es de extrañarse que las nuevas disposiciones establecidas en el Reglamento sean prontamente analizadas, debatidas y discutidas en nuestro país, con el objetivo de seguir adaptándonos a lo que nuestro modelo de referencia ha establecido últimamente.

La segunda razón se vincula con la necesidad de actualizar nuestra ley de datos personales. Sancionada en el año 2000, la ley 25.326 -con todos sus defectos- implicó un fuerte avance en la defensa de los derechos de las personas a la protección de sus datos personales. Sin embargo, el impresionante desarrollo de las tecnologías digitales sucedido con posterioridad dio lugar a la aparición de variados fenómenos que ponen a prueba el actual mecanismo de protección de datos. Por citar algunos casos, la minería de datos ha permitido detectar y elaborar información de un conjunto muy grande de datos en forma automática. Asimismo, las actuales tecnologías de recolección de datos les permiten almacenar gran cantidad de datos acerca de nosotros de forma sencilla y poco onerosa. De esta manera, las empresas pueden comercializar nuestros datos u ofrecernos productos y servicios de acuerdo al perfil que hayan elaborado de nosotros. Asimismo, los gobiernos cuentan con herramientas de vigilancia y a través de diversas tecnologías -como por ejemplo, las tecnologías de biometría, pueden llevar un registro de nuestras actividades cotidianas.

Por lo tanto, es necesario adecuar nuestra legislación para que responda a las potenciales amenazas que el surgimiento de la era digital ha traído a las sociedades del siglo XXI. En esta tarea, resulta útil consultar aquello que se está haciendo en otras partes del mundo. No porque eso implique necesariamente que debamos copiar literalmente lo dicho en otro lado, sino porque siempre es de ayuda saber qué es lo que han estado haciendo países o regiones que ya han dedicado tiempo y recursos al análisis de temáticas que resultan novedosas para nosotros.

Emprender una tarea a partir del conocimiento ya existente es mejor que empezar desde cero. Con este objetivo en mente, es de esperar que este análisis comparativo sirva para plantear los términos de una discusión acerca de las mejores formas de proteger los datos de las personas en un mundo que pareciera volver cada vez más difícil la protección de nuestra privacidad y nuestra intimidad.