Junio 2016

EL FUTURO DE LOS DATOS PERSONALES EN ARGENTINA

Reflexiones de una mesa de trabajo

por los Derechos Civiles

El futuro de los datos personales en Argentina
Reflexiones de una mesa de trabajo*

Presentación

El día 27 de mayo de 2016, la Asociación por los Derechos Civiles llevó a cabo una mesa de trabajo cerrada en la Facultad de Derecho de la Universidad de Buenos Aires (UBA) para debatir el futuro de la protección de datos personales en Argentina. El evento contó con la participación de expertos en protección de datos personales de diversos sectores y se desarrolló en base a dos temáticas principales:

1. Las facultades normativas y operativas del órgano de aplicación de la ley de protección de datos personales.

2. Las posibles consecuencias del nuevo Reglamento General sobre Protección de Datos Personales de la Unión Europea sobre el estatus de Argentina como país con nivel adecuado de protección de datos personales.

Asimismo, en cada uno de los segmentos de debate, se abordó el manejo de bases de datos por parte del Estado, ya que se trata de una temática que influye en la discusión y análisis de los temas debatidos.

*El presente documento fue elaborado por Jeannette Torrez y Eduardo Ferreyra de las áreas de Privacidad y Libertad de Expresión de la Asociación por los Derechos Civiles. El contenido de este documento no refleja la opinión de ADC, a menos que así se indique en forma expresa. El mismo se encuentra bajo una licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional, de difusión pública y sin fines comerciales.

Durante el encuentro se acordó aplicar la regla de Chatham House, por lo que este documento reflejará los puntos centrales de la discusión sin individualizar a sus participantes, intentando reproducir de la manera más fiel posible el diálogo ocurrido.

Breve introducción al sistema de protección de datos personales

- Argentina posee la ley 25.326 de protección de datos personales desde el año 2000.[1]

- La ley argentina está inspirada en la española "Ley orgánica de regulación del tratamiento automatizado de datos" (LORTAD) de 1992,[2] que posteriormente fue derogada por la Ley orgánica de protección de datos de carácter personal.

- Nuestro sistema se inspira en el modelo europeo, que a través de su Directiva de Protección de Datos Personales 95/46/EC[3] y el actual Reglamento General 2016/769[4] establece una regulación integral sobre todos lo sectores involucrados en el tratamiento de datos personales. En este sentido, se diferencia del sistema norteamericano, en el cual la regulación se realiza por sectores y por ende, no existe una legislación general sobre protección de datos.

- El órgano de aplicación de la ley de datos personales es la Dirección Nacional de Protección de Datos Personales (DNPDP), creada en el año 2001.[5]

- Grupo de Trabajo del Artículo 29, Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina, 3 de octubre de 2002.[6]

[1] http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
[2] http://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189
[3] http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=ES
[4] http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES
[5] http://www.jus.gob.ar/datos-personales.aspx
[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp63_es.pdf

- 2003/490/CE: Decisión de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.[7]

El impacto del nuevo Reglamento General de Protección de Datos de la UE en Argentina

La Directiva Europea de Protección de Datos de 1995 sienta el principio general en materia de transferencia internacional de datos. Este principio establece que los datos personales de los ciudadanos de la Unión Europea (UE) no pueden ser transferidos a terceros países, si éstos no garantizan un nivel adecuado de protección.

La Comisión Europea es el órgano encargado de decidir si un país posee un nivel adecuado de protección de los datos personales. El procedimiento para llegar a esa decisión es el siguiente: primero se realiza una investigación independiente por parte de un grupo académico; luego, tanto el grupo de trabajo del art. 29 (compuesto por un representante de la autoridad nacional de protección de datos de cada país miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea) como el Comité del art. 31 emiten un dictamen, y finalmente la Comisión emite una decisión.

El atentado terrorista a las Torres Gemelas del 2001 cambió el modo en que se analizaba la transferencia internacional de datos. Antes del ataque, predominaba un enfoque de derecho privado y lo que importaba eran las transferencias entre empresas. Luego de 2001, se empieza a analizar la temática desde una perspectiva de derecho público y los tratamientos que realizan los Estados.

En 2009 se adopta la Carta de Derechos Fundamentales de la Unión Europea,[8] que incorpora como derecho fundamental la protección de datos personales. Esto va a producir un impacto grande en la forma de regular la problemática, ya

[7] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003D0490&from=EN
[8] http://www.europarl.europa.eu/charter/pdf/text_es.pdf

que hasta ese momento la protección de datos era considerado un tema de mercado interior. Al ser considerado ahora un derecho fundamental, los niveles de protección requeridos a los terceros países serán más altos.

La influencia de la Carta de Derechos Fundamentales se hizo ver en la sentencia del caso "Schrems",[9] en el cual el Tribunal de Justicia de la Unión Europea declaró la nulidad del Safe Harbor[10] (conjunto de principios a los cuales las empresas estadounidenses debían adherir para recibir datos de los países de la UE).

En el 2014 se producen las revelaciones de Snowden,[11] y a partir de estas revelaciones queda claro que el sector público –particularmente la Agencia de Seguridad Nacional (NSA por su nombre en inglés)– podían acceder a todos los datos de las empresas privadas de los grandes gigantes de Internet, muchos de los cuales provenían de la Unión Europea.

El ciudadano Schrems hace el análisis de que Facebook Irlanda transfería sus datos a EEUU vía Safe Harbor. No obstante, cuando estos datos llegaban a EEUU, en todo lo que era el acceso de la NSA a esos datos recibidos por Facebook no había protección, porque no se contaba con los derechos básicos de protección de datos (no había derecho a acceso, derecho a un recurso judicial, no existía una autoridad independiente de control) Schrems plantea una queja ante la autoridad, la cual es rechazada. Schrems apela y el caso llega hasta la Corte Suprema de Irlanda. Como se trata de una cuestión de derecho europeo, la Corte de Irlanda remite una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea (TJUE).

El TJUE decide invalidar el Safe Harbor porque considera que dicho acuerdo no garantiza un nivel "esencialmente equivalente" de protección. Por "esencialmente equivalente" se entiende que el tercer país debe respetar los principios básicos que contiene la Carta de Derechos Fundamentales de la UE.

El nuevo Reglamento General de Protección de Datos[12] refuerza la tendencia protectoria: se incluye la referencia "esencialmente equivalente" en los considerandos

[9] Sentencia del Tribunal de Justicia: Maximillian Schrems v. Data Protection Commissioner

[10] https://www.ftc.gov/tips-advice/business-center/guidance/federal-trade-commission-enforcement-us-eu-us-swiss-safe-harbor

[11] http://www.cjfe.org/snowden

[12] http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

del Reglamento, se agregan ciertos requisitos para el análisis de adecuación en el capítulo V referente a transferencias internacionales, y se incluye un aspecto que va a tener un impacto directo en Argentina y todos los países declarados adecuados, que es la obligatoriedad para la Comisión Europea de realizar análisis periódicos respecto del nivel de adecuación.

Con el nuevo Reglamento la Comisión va a estar obligada a realizar este análisis periódico, con lo cual Argentina va a ser reevaluada antes del año 2022. El reglamento entra en vigencia en 2018 y su texto dice que esta reevaluación va a tener que tener lugar al menos cada cuatro años, con lo cual es ineludible que va a llegar un momento en el cual Argentina va a ser sometida a esta evaluación.

El hecho de que la ley 25.326 no requiera el consentimiento para los tratamientos que realiza el Estado no quiere decir que el Estado está exento para cumplir con la legislación. Incluso la rigidez es mayor: que la Policía no tenga la obligación de informar o dar acceso si hay un riesgo en la investigación no significa que no tenga que cumplir. En todo caso dará más tarde la información cuando ya no esté el riesgo. Si una persona pide acceso a sus datos y el poder de policía no puede dar acceso en ese momento, va a tener que intervenir la autoridad de protección de datos haciendo un acceso indirecto.

La consagración del derecho a la protección de datos personales como un derecho fundamental se expresa a través del art. 8 de la Carta Fundamental. En base a este principio, se realizan todos los análisis actuales en materia de adecuación, en particular la sentencia del caso "Schrems" y el informe del grupo del art. 29 sobre el proyecto de Privacy Shield,[13] acuerdo que busca reemplazar al Safe Harbor.

La directiva anterior exigía también un nivel adecuado de protección. Entonces Estados Unidos, al saber que su sistema jurídico difícilmente iba a ser aceptado, empieza a trabajar en la creación de los principios del Safe Harbor a los cuales las empresas pueden adherir. Cuando la Corte Europea invalida el Safe Harbor, no es que no pueden hacer más transferencias, ya que el razonamiento es el siguiente: si no es adecuado se pueden aplicar excepciones de aplicación restrictiva, no pueden aplicarse al consentimiento cuando la transferencia es estructural o sistemática

[13] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

y para esos casos el responsable del tratamiento puede dar garantías de que el que reciba esos datos va a aplicar medidas de protección. Estas son las cláusulas contractuales tipo u otro medio que se llaman "Binding Corporate Rules",[14] que son más que nada para las multinacionales. Cuando sucede lo del Safe Harbor las empresas empezaron a redactar contratos para que se puedan seguir haciendo las transferencias. Ahora la discusión es política: la Comisión Europea está negociando con Estados Unidos un nuevo marco, que se va a llamar Privacy Shield[15] y el grupo del art. 29 emitió un dictamen donde critica ciertos aspectos de este acuerdo. Sin embargo, se trata de una negociación política.

La nueva directiva europea establece que el lenguaje debe ser claro, entendible y breve. No se consideran válidas los textos de grandes cantidades de páginas y escritos con un lenguaje técnico que suelen figurar en las políticas de protección de datos de las empresas e instituciones. A su vez, el tipo de tratamiento determinará la naturaleza de la información: si no se trata de datos invasivos, bastará un aviso en el sitio web. Por el contrario, si son datos sensibles, la persona debe recibir en papel la información, además de la que figure en el sitio web.

Existen varias consecuencias que sucederían si Argentina llegara a perder el status de país con nivel adecuado de protección de datos. En primer lugar, está la reputación. Para la imagen internacional del país, sería un gran retroceso, ya que gozar de dicho estatus es un bien intangible, que está reconocido en el ámbito internacional. Por otro lado, el país se vería dificultado de realizar acuerdos de transferencia de datos con otros países, por ejemplo, en materia de cooperación por temas de seguridad. Asimismo, no existiría libre circulación del flujo de dato, con lo cual se incrementarían los costos para aquellas empresas que deseen hacer transferencias de datos con Argentina. Podrían generarse conflictos con tratados comerciales, ya que se ofrecería un estándar muy bajo de protección y todos los contratos deberían ser renegociados.

Existen ciertos estándares de la normativa europea que pueden entrar en conflicto con los estándares del sistema interamericano de derechos humanos. Un ejemplo

[14] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

[15] El acuerdo de Privacy Shield fue aprobado por la Comisión Europea con posterioridad a la realización de la presente mesa de trabajo

de ello es el derecho al olvido, el cual no está resuelto de manera unánime en el continente. Todavía la compatibilidad del derecho al olvido con la Convención Americana es una cuestión compleja, sobre la que todavía no se ha dado una discusión abierta y franca.

Con el tema del derecho al olvido, existe una visión parcial del régimen europeo. Respecto a la sentencia en el caso Google, no siempre se llega hasta el final de la resolución, en donde se dice que el derecho al olvido no es un derecho absoluto, sino que tiene que ser aplicado caso por caso y que en determinados casos no se va a aplicar –por ejemplo cuando esa persona es pública o cuando hay un interés público en que esos datos se conozcan–. Esos mismos principios están en el nuevo Reglamento.

Protección de Datos Personales en Argentina

Argentina, es uno de los pocos países que ha recibido certificación de la UE considerando adecuada la Ley de Protección de Datos Personales[16], no obstante, ello no fue un cheque en blanco, y requiere un proceso de recertificación. De acuerdo a este proceso, es necesario empezar a reflexionar cuáles serían los cambios necesarios en la legislación para mantener a la Argentina como país adecuado. La Dirección Nacional de Protección de Datos Personales es uno de los impulsores en el proceso de reflexión sobre la necesidad de la reforma de la Ley 25.326.

[16]Argentina fue certificada como país adecuado en 2003, ver 2003/490/CE: Decisión de la Comisión, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina. Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes países: Suiza: Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000 Canadá: Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos Guernsey: Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003 Isla de Man: Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004 Jersey: Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008 Islas Feroe: Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010 Andorra: Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010 Israel: Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011 Uruguay: Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012 Nueva Zelanda: Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012

Es importante mencionar que la Dirección Nacional de Protección de Datos Personales actualmente se encuentra enfrentando dos desafíos, el primero busca reorientar la labor de la Dirección y el segundo se relaciona con el proceso de reflexión mencionado anteriormente.

La "reorientación" de la labor de la DNPDP hace referencia a que la misma estará mayormente vinculada con tareas de control en detrimento de tareas relacionadas con capacitación, difusión y educación. Si bien cuando la ley 25.326 fue aprobada en el año 2000 era fundamental realizar una tarea de concientización y sensibilización frente a una nueva reglamentación, sin embargo, luego de 15 años de esta tarea se vuelve necesario preguntarnos cuál debe ser la actividad principal de la DNPDP.

Cuando se habla de reorientación, se remite a que la DNPDP intentará enfocar sus tareas en los procesos de control, desde las inspecciones hasta los procesos de sumarios sancionatorios. La DNPDP tiene posibilidades de iniciar acciones de inspecciones o investigaciones de oficio, por denuncias y actualmente, se encuentra trabajando para agilizar este proceso, pudiendo hacer en algún momento más públicas dichas cuestiones. En la actualidad, existen trámites burocráticos que retrasan los procesos de detección de infracciones, por ejemplo, cuando la Dirección detecta irregularidades y decide evaluar una determinada sanción, necesariamente su función sancionatoria tiene también una revisión por parte del Departamento de Asuntos Jurídicos del Ministerio de Justicia. Aún incluso cuando la DNPDP agilice este proceso y queden firmes tipos de distintas sanciones económicas, el proceso de ejecución de una multa administrativa, para cualquier órgano, es un proceso extenso en el que interviene el Estado Nacional contra los particulares que no han pagado una multa.

Cuando se menciona la reorientación del trabajo de la Dirección, no significa que se va a abandonar todo tipo de trabajo de capacitación o difusión, lo que se busca es combinarlo con organizaciones gubernamentales y no gubernamentales para que colaboren en estos procesos en vez de que la DNPDP los lidere. El objetivo es que la Dirección empiece a ejercer un rol más activo como órgano de control, aún incluso resignando la obligación del registro de bases de datos, dado que dicho instrumento crea una ilusión de control y no necesariamente

logra cumplir la finalidad que persigue. Las estadísticas indican que el total de multas y apercibimientos desde que se creó hace 15 años la DNPDP es 85, lo que indica que éste no ha sido un órgano que ha perseguido los problemas que hay en el tratamiento de datos, de este total 69 son multas, de las cuales 5 se pusieron entre 2005 y 2010 lo cual marca claramente la orientación de la oficina, entre 2010 y 2016 hay un incremento de 64. Hay un 56% que han sido pagadas, sin embargo, existe un inconveniente en el monto de las multas debido a un problema legal de regulación normativa, ya que los montos están creados por ley y no tienen disparadores de actualización.

Por otro lado, una vez que han sido impuestas o hechas inspecciones o bien detectado infracciones la Dirección tratará de hacer transparente y pública esta situación, haciendo de público conocimiento que una empresa ha sido multada por una infracción, en ese punto es donde la sociedad civil puede colaborar, promoviendo la actividad que está haciendo la DNPDP en su función de órgano de control.

Otra cuestión que se inserta en la reorientacion de las tareas de la DNPDP, está relacionada con enfrentar el enorme desafío interno de abordar el control de cierto tratamiento de datos. Nos referimos a los problemas relacionados con Big Data, y a los cuales, la Dirección tiene intención de abordar bajo un enfoque distinto al habitual, bajo el cual solo se pueden controlar bases de datos registradas, abriendo la posibilidad de iniciar investigaciones si se advirtieran violaciones a la ley por parte de aplicaciones. Si bien esto es un proceso complejo para cualquier autoridad de datos personales en el mundo, debido a los problemas legales vinculados con jurisdicción, la DNPDP tiene intención de generar discusiones e intervenir en función de la ley y las capacidades que tiene. En muchas ocasiones,el registro crea una ilusión de que efectivamente se está cumpliendo con la ley, sin embargo, esto puede generar situaciones injustas, por ejemplo cuando se decide llevar adelante inspecciones, éstas se realizan sobre la base de los que están registrados. Si bien la Dirección aún no está proponiendo la eliminación del registro, si promueve tener este debate que ya se está discutiendo a nivel internacional.

Como fue mencionado anteriormente, existe el desafío de iniciar el proceso de

reflexión de reforma de la ley 25.326, en el cual pueda ponerse en discusión cómo nuestra ley protege datos personales en el contexto actual de vertiginoso avance de la tecnología.

La protección de datos es un tema de agenda mundial y no es casual que gran parte de la discusión entre la Unión Europea y Estados Unidos esté concentrada en protección de datos y protección de la privacidad debido a que tiene que ver con problemas de vigilancia y de comercio. Cuando se habla de vigilancia nos referimos en lo que tiene que ver con la lucha contra el terrorismo y el crimen organizado, es decir, en cómo los Estados quieren muchas veces bienintencionadamente, avanzar sobre determinadas investigaciones que pueden poner en peligro la privacidad. Y cuando hablamos de comercio internacional nos referimos a que el comercio internacional es en gran medida comercio electrónico, en ese sentido en la discusión global, el cambio de reglas va a impactar en Argentina y en América Latina, si es positivo o no restará evaluarlo.

Como se mencionó, una de las limitaciones de la DNPDP se vincula con la jurisdicción. Por cuestiones de la organización constitucional federal, la labor de control de la Dirección en bases de datos registradas o tratamiento de datos a nivel provincial, puede resultar perjudicada. El principal inconveniente es que se podría derivar en una situación injusta en el sentido que la Dirección controle a quienes están registrados en la Región Metropolitana de Buenos Aires a donde simplemente se puede llegar físicamente. No obstante, aún cuando se tuvieran recursos para llegar a las Provincias existirían limitaciones legales, es decir, por más que se tuvieran recursos para tener un cuerpo de inspectores a nivel nacional muchas cosas no podrían realizarse por limitaciones legales. Esto se vislumbra como lo más pedestre acerca de cómo la DNPDP puede actuar como órgano de control según la ley actual.