Impacto en Uruguay del nuevo Reglamento de la Unión Europea sobre protección de datos personales

María Verónica Pérez Asinari[1]

[1] Jefa de la Unidad de Supervisión y Aplicación de la Ley de la Oficina del Supervisor Europeo de Protección de Datos.

El 4 de mayo de este año se publicó en el Diario Oficial de la Unión Europea el Reglamento 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de los datos personales de las personas físicas. Este texto será aplicable a partir del 25 de mayo de 2018. También se adoptó la Directiva del Parlamento Europeo y del Consejo a propósito de la protección de los datos personales de las personas físicas por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

En la Unión Europea (UE), la protección de los datos personales de las personas físicas es un derecho fundamental. Es claro que los cambios tecnológicos y la globalización traen aparejados nuevos desafíos relacionados con este derecho y otros que se encuentran conectados, como por ejemplo, el derecho a la intimidad (sobre todo si se considera el impacto de internet en la vida cotidiana de las personas) y el tratamiento de nuestros datos personales por parte del Estado y las empresas.

Se trata de una reforma emblemática, que trae aparejados cambios sustanciales: refuerza los derechos de los individuos, facilita su ejercicio, enfatiza la responsabilidad de los organismos públicos y las empresas de documentar internamente las medidas adoptadas para cumplir con la legislación y fortalece el poder de las autoridades independientes de protección de datos, incluyendo multas que pueden alcanzar el 4% de la facturación global de una empresa.

Dentro de las reformas que presenta el nuevo reglamento hay dos aspectos que tienen un impacto directo en Uruguay: a) la adecuación para la transferencia internacional de datos personales y b) la nueva delimitación del ámbito de aplicación territorial, así como su dimensión extraterritorial.

a) La adecuación y los flujos transfronterizos de datos personales

La legislación europea en materia de protección de datos establece que la información relativa a los individuos (datos personales) solo puede ser transferida a un país no miembro de la UE cuando ese país asegure un nivel de protección adecuado. Se considera que un país otorga un nivel de protección adecuado cuando su sistema legal y el modo en que este es aplicado en la práctica garantizan determinados derechos y obligaciones que son considerados esenciales en la UE. Entre estos, se destacan los principios de limitación de finalidad, proporcionalidad, calidad de los datos, transparencia y seguridad; los derechos de acceso, rectificación y oposición; las restricciones respecto de transferencias sucesivas a otros terceros países y los mecanismos adecuados de procedimiento y control. Dichos mecanismos contemplan

estándares como la protección de datos por parte de una autoridad independiente, un nivel satisfactorio de cumplimiento, el apoyo y la asistencia a los interesados y la existencia de vías adecuadas de recurso. Si el país de destino de los datos no es adecuado, habrá que evaluar si es aplicable alguna excepción, como por ejemplo, consentimiento del titular, necesidad para un contrato, interés vital o razones importantes de interés público. En caso de que las excepciones no procedan, la transferencia solo podrá tener lugar si la organización presenta garantías suficientes sobre el nivel de protección que ofrece el destinatario de los datos, como por ejemplo, la firma de cláusulas contractuales.

La Comisión Europea puede adoptar una decisión que declare que un país no miembro de la UE garantiza un nivel adecuado de protección. Cuando ello sucede, se establece el libre flujo de datos personales entre la UE y ese país no miembro o un sector de un tercer país. Ello incluye un análisis pormenorizado de la letra de la ley y de la realidad en su aplicación. Hasta la fecha, muy pocos países han obtenido tal calificación por parte de la Comisión Europea. Uruguay se encuentra en ese pequeño grupo de países que han sido declarados "adecuados".[2] Los otros son Suiza, Argentina, Israel, Nueva Zelanda, Andorra, Guernsey, Jersey, Isla de Man, Islas Feroe y un sector de Canadá (sector privado). Estados Unidos contaba con un sistema, conocido como *Safe Harbor*, que cubría solo las empresas que autocertificaban el cumplimiento de determinados principios. No obstante, un fallo de la Corte de Justicia de la UE de 2015 anuló la decisión de la Comisión que declaraba el *Safe Harbor* "adecuado"[3].

La decisión de adecuación no significa un "cheque en blanco", sino que la comisión siempre estuvo facultada para revisar el sistema del país no miembro, su aplicación y la incidencia en la decisión de adecuación. No obstante, hasta el momento no se han realizado revisiones formales respecto de los países declarados adecuados. Con la adopción del nuevo reglamento se produce un cambio importante,[4] ya que la Comisión Europea deberá realizar revisiones periódicas, al menos cada cuatro años, que tengan en cuenta los desarrollos acaecidos en los países declarados adecuados. Si la revisión revelara que alguno de esos países no sigue asegurando un nivel adecuado de protección, la comisión deberá decidir en ese sentido y, hasta donde fuese necesario, repeler, enmendar o suspender la decisión de adecuación. La comisión deberá consultar al país de que se trate con el objeto de remediar una situación tal. Es

[2]En Uruguay, la materia es regulada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Hábeas Data.

[3]La Corte consideró que tal decisión no garantizaba la protección de los derechos fundamentales a la intimidad y a la protección de datos personales. Se trata del caso Schrems (C-362/14), basado en las transferencias realizadas por Facebook desde la UE a EE.UU., considerando el impacto de las revelaciones de Snowden en la protección de los derechos fundamentales.

[4] Artículo 41 del Reglamento.

por ello que los países que quieran conservar la adecuación deberán asegurarse que el nivel de protección continúe siendo satisfactorio y que sea acorde a los desarrollos “esenciales” de la materia en la UE. De ese modo, se deberá considerar el impacto de la adopción de la Carta de Derechos Fundamentales y del nuevo reglamento, así como la jurisprudencia europea; tal es el caso Schrems, en el cual la Corte de Justicia de la Unión Europea refuerza el concepto de adecuación al requerir que el nivel de protección sea “esencialmente adecuado”.

b) Ámbito de aplicación territorial

El nuevo reglamento se aplicará a las organizaciones y empresas que se encuentren establecidas en el territorio de la UE y a aquellas que no se encuentren establecidas en el territorio de la UE cuando las actividades de tratamiento estén relacionadas con:

-La oferta de bienes o servicios a individuos en la UE, independientemente de si a estos se les requiere su pago.

-El control de su comportamiento, en la medida de que este tenga lugar en la UE.[5]

Es por ello que una empresa uruguaya (por ejemplo, una app o un sitio web) que ofrezca bienes o servicios a individuos en la UE o que controle su comportamiento, deberá cumplir con el nuevo Reglamento de Protección de Datos. Y esto no solo implica cumplir con las obligaciones y respetar los derechos de los individuos, sino también designar un representante en la UE, salvo que la actividad de tratamiento de datos personales sea ocasional.

[5] Artículo 3.2 del Reglamento.