El acuerdo de Puerto Seguro

POR **ALFONSO ORTEGA GIMÉNEZ**

Las relaciones entre los Estados Unidos y la Unión Europea en materia de protección de datos de carácter personal no atraviesan su mejor momento, lo cual se traduce en la falta de confianza en las transferencias internacionales entre dichos Estados. El siguiente artículo trata de aportar algo de luz al problema abordando dos cuestiones clave: el sistema estadounidense de Principios de Puerto Seguro para la protección de la vida privada y la reconstrucción del marco normativo de la protección de datos en la UE.

La Directiva 95/46/CE supuso el inicio de una disputa entre la Unión Europea y los Estados Unidos, puesto que posibilitaba que las exportaciones de datos de carácter personal a los EEUU fueran prohibidas, ya que, mientras el enfoque estadounidense en esta materia se basaba en una mezcla de legislación, reglamentación y autorregulación, la UE consideraba imprescindible la protección del derecho fundamental a la privacidad.

Transferencias internacionales de datos de carácter personal a entidades ubicadas en EEUU

Tras largas negociaciones, el 29 de julio de 2000 la UE y EEUU llegaron a un acuerdo, denominado *Safe Harbour Principles* (Principios de Puerto Seguro), por el que se establecía un sistema para la protección de la vida privada, una auténtica suerte de extensión de la regulación vigente en la UE en materia de protección de datos de carácter personal. Se trataba de un sistema eficaz tanto desde el punto de vista teórico como desde el práctico, ya que posibilita un flujo estable e ininterrumpido de información asegurando un nivel permanente de protección adecuado.

El sistema de Principios de Puerto Seguro, aunque ha sido criticado en algunas ocasiones, presenta numerosas ventajas, teniendo en cuenta que: constituye un marco normativo uniforme, permanente, estable y definitivo para la protección del derecho a la intimidad y para la transferencia internacional de datos de carácter personal entre la UE y los EEUU; permite la aprobación automática por todos los Estados miembros de la UE de las transferencias internacionales de datos de carácter personal con destino a los EEUU y sustituye las

Fundación Telefónica
Telefónica

legislaciones internas de cada uno de los Estados miembros de la UE.

La razón de ser de los Principios de Puerto Seguro es el hecho de que EEUU se rige, en numerosos ámbitos, por el principio de autorregulación, en virtud del cual son las propias empresas las que adoptan sus códigos de conducta o se acogen a códigos de conducta sectoriales, respecto de los cuales el Estado carece de facultad fiscalizadora o de control alguno. Para suplir esta laguna se crean los principios de *Safe Harbour*, un sistema que trata de conjugar la autorregulación estadounidense con el régimen jurídico comunitario europeo en esta materia.

La empresa que se quiera adherir a este sistema deberá presentar una carta de autocertificación ante el Departamento de Comercio, por la que manifieste su adhesión a los Principios y FAQ, así como indicando, en particular, los datos de identificación de la entidad solicitante, una descripción de su actividad en lo relativo a la información personal recibida de la UE y una descripción de su política de protección de datos de carácter personal.

El sistema de Principios de Puerto Seguro se configura, entonces, como un programa voluntario, basado en la autocertificación y en la autoevaluación, que se ofrece a las entidades estadounidenses con el fin de obtener respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida en el ámbito comunitario, que permite asegurar de manera permanente la legitimidad de las transferencias internacionales de datos de carácter personal.

Principios de Puerto Seguro

Los Principios de Puerto Seguro, que se configuran como mínimos para cualquier política privada de protección de datos de carácter personal, son los siguientes:

– Principio de Notificación (*Notice*): establece la obligación que tienen las entidades de informar a los particulares de los fines y utilización de sus datos de carácter personal.

– Principio de Opción (*Choice*): dispone la obligación de las entidades de ofrecer a los particulares la posibilidad de decidir si sus datos de carácter personal pueden ser o no cedidos a un tercero.

– Principio de Transferencia Ulterior (*Onward Transfer*): señala que para revelar información a terceros que no participen en el sistema de Puerto Seguro, las entidades deberán aplicar los Principios de Notificación y de Opción.

– Principio de Seguridad (*Security*): establece que las entidades que se encargan de la recogida de datos de carácter personal deberán tomar todas las precauciones que estimen oportunas con el fin de evitar la pérdida, modificación o destrucción de los mismos.

– Principio de Integridad de los datos (*Data Integrity*): señala que los datos de carácter personal deben ser pertinentes con respecto a los fines con los que se utilizan.

Fundación Telefónica
Telefónica

– Principio de Acceso (*Access*): recoge el derecho de los particulares al conocimiento de los datos de carácter personal que las entidades tengan sobre ellos y poder corregirlos, modificarlos o suprimirlos en caso de que sean inexactos.

– Principio de Aplicación (*Enforcement*): dispone la necesidad de incluir una vía de recurso para los interesados que se vean afectados por el incumplimiento de la normativa sobre transferencia internacional de datos de carácter personal entre los EEUU y la UE.

Sin embargo, existe toda una serie de excepciones a estos Principios: cuando sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley, cuando una disposición legal o resolución jurisdiccional así lo establezca y/o cuando la Directiva 95/46/CE o cualquier norma de los Estados miembros de la UE lo permita, en cumplimiento de la Directiva 95/46/CE, las entidades estadounidenses pueden adoptar cualquiera de las siguientes posturas: adherirse al sistema de Principios de Puerto Seguro; acudir a fórmulas que exoneren del requisito de la protección adecuada, que recoge el artículo 26 de la Directiva 95/46/CE, o no recibir datos de carácter personal de la UE.

Ante el incumplimiento por parte de las entidades estadounidenses del sistema de Puerto Seguro, caben dos posibilidades:

– La suspensión de las transferencias de datos de carácter personal hacia una entidad que haya autocertificado su adhesión a los Principios y su aplicación de conformidad con las FAQ, con el fin de proteger a los particulares de un 'tratamiento fraudulento' de sus datos de carácter personal, o la adopción de cualquier otra medida dentro de sus competencias con el fin de evitar ese tratamiento fraudulento de los datos de carácter personal de los particulares, o

– Si se demostrara que un organismo encargado del cumplimiento de los Principios de Puerto Seguro en los EEUU no está ejerciendo su función, la Comisión Europea notificará al US Department of Commerce su intención de adoptar toda una serie de medidas con el objeto de anular, suspender o restringir la transferencia internacional de datos de carácter personal entre los EEUU y la UE.

Puntos débiles del acuerdo

En cuanto al ámbito del acuerdo UE-EEUU, es preciso especificar varios extremos:

– Si se excluyen algunos sectores del ámbito del mecanismo de Puerto Seguro en virtud de disposiciones especiales (por ejemplo, el sector público) o por la inexistencia de un organismo público de supervisión con responsabilidad para ocuparse de la cuestión.

– Si la entidad podrá, cuando notifique su adhesión al Puerto Seguro, excluir algunos sectores de su propia actividad (por ejemplo, los servicios en línea) y cómo se hará pública y se pondrá tal exclusión en conocimiento de las autoridades nacionales de control.

– Respecto de las transferencias de datos de trabajadores, reforzar el nivel general de

Fundación Telefónica
Telefónica

protección que brindan los principios o excluir dichos datos del ámbito de aplicación de los acuerdos para proporcionarles mayor protección, en vista asimismo de la inexistencia de un organismo público independiente capaz de ocuparse de este tipo de datos.

– No introducir excepciones a la aplicación de los principios recurriendo a la regulación y sin tomar en la debida cuenta los intereses de la protección de la intimidad.

Además, respecto de las condiciones de aplicación e imposición del acuerdo, varias son las cuestiones que nos asaltan: ¿Qué repercusión tendrá en la función de las autoridades nacionales de control la elección de una sociedad estadounidense con quejas incursas ante un organismo específico?; en el ámbito europeo, cuando se tramiten las quejas, ¿cuáles serán las competencias respectivas de las autoridades nacionales de control y de la UE?; en el caso de procedimientos que tengan lugar en EEUU y en la UE de manera simultánea o sucesiva y que resulten en posturas contrarias respecto de una misma queja, ¿cómo se resolverán las diferencias?

Finalmente, sobre el contenido de los Principios de *Safe Harbour*, pensamos que se debería poner la atención, en particular, en alguno de ellos: por un lado, sería aconsejable reforzar el Principio de Opción, ya que los principios de Puerto Seguro no regulan la legitimidad de los criterios de tratamiento; y, por otro lado, respecto del Principio de Acceso, pensamos que las excepciones que contienen las FAQ son demasiado generales, que es preciso abarcar los datos públicos, y que los datos cuyo tratamiento vulnere los Principios habrán de corregirse o suprimirse.

La necesaria aplicación trasnacional del Derecho de la UE en protección de datos

El mundo se encuentra dividido en tres grandes grupos en materia de regulación de la protección de datos de carácter personal: un primer grupo, formado por los Estados donde existe legislación en materia de protección de datos; el segundo grupo, el formado por aquellos países en los que se está trabajando en pro de una legislación en materia de protección de datos y, finalmente, un tercero, el integrado por aquellos países donde la legislación en materia de protección de datos, de momento, brilla por su ausencia.

Pues bien, la UE debe actuar; su Derecho en protección de datos debe no solo vincular a los Estados del primer grupo, sino que debe aspirar a convertirse en ‘fuente de inspiración’ para los del segundo y tercer grupo. Así, conseguiremos que el derecho de la UE en protección de datos sea de aplicación dentro y fuera de la UE.

No obstante, para garantizar el funcionamiento del mercado interior y favorecer el diálogo y las relaciones comerciales entre la UE y terceros Estados, debemos aproximar la Directiva 95/46/CE a la nueva realidad social y tecnológica que hoy día vivimos, convirtiendo ese Derecho de la UE en materia de protección de datos en un motor efectivo en la armonización de la normativa de la UE y en la promoción de su carácter universal.

El marco normativo de la protección de datos en la UE tiene, sin duda alguna, un impacto (que no un ámbito) extraterritorial real: se extiende más allá de las fronteras comunitarias. La

Fundación Telefónica
Telefónica

creación de un ‘mercado interior de datos de carácter personal’ y la apuesta por la ‘libre circulación de datos personales’ han sido posibles gracias a que las legislaciones estatales se han unificado a través del desarrollo de una norma común -un Derecho unificado en materia de protección de datos para todos los Estados miembros de la UE- que ha permitido: *ad intra*, la libre circulación de datos -tan necesaria para la realización del mercado interior y el desarrollo del comercio internacional- y no restringida *ad extra* -Acuerdos entre la UE y terceros Estados-; eso sí, sin constituir una barrera ‘disfrazada’ al comercio internacional.

Riesgos y desafíos de la normativa

La preocupación comunitaria por evitar una deslocalización masiva de ficheros de datos y la creación de ‘paraísos de datos’, junto con una cierta preocupación existente por la posible utilización del Derecho de la UE en protección de datos como una barrera al comercio internacional con terceros Estados, debe llevarnos a un marco jurídico que no sea artificioso desde el punto de vista técnico y cuya implementación práctica no sea de gran dificultad. La apuesta debe ser clara: por un lado, una mejora de los actuales mecanismos de transferencia internacional de datos a terceros Estados, que incluya decisiones de adecuación; y por otro lado, la articulación de unas garantías apropiadas para, valga la redundancia, garantizar un alto nivel de protección de datos en las operaciones internacionales de tratamiento de datos y facilitar el flujo transfronterizo de los mismos.

El desafío es claro: reconstruir el Derecho de la UE en protección de datos para consolidarlo con un marco jurídico moderno, rápido, económico, eficaz, coherente, de aplicación trasnacional (no solo territorial, sino también extraterritorial), global y dirigido no solo a los Estados miembros de la UE sino también a terceros Estados. En definitiva, un Derecho de la UE en protección de datos sólido y coherente, que potencie la dimensión de mercado único de la protección de datos y favorezca las relaciones comerciales entre la UE y terceros Estados.

El incremento de las transferencias internacionales de datos personales implica la necesidad de que los Estados reaccionen restringiendo la captura, procesamiento y diseminación de los mismos. Son varios los retos a los que nos enfrentamos:

– El incremento en la subcontratación del tratamiento -muy a menudo fuera de la UE-, que plantea varios problemas vinculados a la legislación aplicable al tratamiento y a la atribución de la responsabilidad correspondiente.

– La necesidad de clarificar y simplificar las normas aplicables a las transferencias internacionales de datos personales, con el fin de evitar el riesgo de que el nivel de protección de los interesados previsto en un tercer país se juzgue diferentemente de un Estado miembro a otro.

– La conveniencia de reforzar el papel de las autoridades de control encargadas de la protección de datos, con el fin de mejorar la aplicación de las normas en el ámbito de las transferencias internacionales de datos.

– O la necesidad de disponer de un instrumento global, aplicable a las operaciones de

Fundación Telefónica
Telefónica

tratamiento de datos en todos los sectores y políticas de la UE, que garantice un enfoque integrado y una protección global, coherente y eficaz.

Divergencias en la interpretación de la norma entre los Estados miembros de la UE

Hoy día no se puede identificar la UE como el espacio geográfico en el que se procura al individuo una mayor defensa de sus datos personales, ya que las divergencias entre las legislaciones de los Estados miembros sobre la aplicación del régimen de la UE en materia de transferencia internacional de datos (artículos 25 y 26 de la Directiva 95/46/CE) son excesivas.

El planteamiento adoptado por algunos Estados, en los que se considera que es el responsable del tratamiento de datos quien tiene que evaluar la adecuación de la protección prestada por el destinatario, con un control muy limitado de los movimientos internacionales de datos por parte del Estado o la autoridad nacional de control, no parece cumplir el requisito impuesto a los Estados miembros en el apartado 1 del mencionado artículo 25.

Existe una necesidad acuciante de modernizar las normas de exportación de datos, en pro de la mencionada libre circulación de datos de carácter personal. Como mínimo, la reforma debe garantizar: una verdadera prueba de adecuación; la atención debe centrarse en las prácticas empresariales y no en normas teóricas, y debe existir un ámbito para la certificación por parte de terceros.

El futuro debe pasar por la necesaria simplificación de los requisitos para las transferencias internacionales de datos personales, lo cual implicaría la apuesta por:

– Un recurso más amplio a la constatación de la protección adecuada en relación con terceros países con arreglo al apartado 6 del artículo 25 de la Directiva 95/46/CE.

– La adopción de nuevas Decisiones con arreglo al apartado 4 del artículo 26, de manera que los agentes económicos cuenten con una gama más amplia de cláusulas contractuales tipo.

– Reforzar el papel de las normas empresariales vinculantes para brindar las garantías adecuadas a las transferencias de datos personales dentro del grupo y

– Una interpretación más uniforme del apartado 1 del artículo 26 de la Directiva.

El planteamiento adoptado por algunos otros Estados miembros, que someten todas las transferencias a terceros países a una autorización administrativa, también parece incoherente con el objetivo mismo de la Directiva 95/46/CE: garantizar la protección adecuada y al mismo tiempo las transferencias internacionales de datos personales a terceros países sin obligaciones innecesarias.

Con arreglo al artículo 19 de la Directiva 95/46/CE, pueden exigirse notificaciones a las autoridades nacionales de control, pero estas no pueden convertirse, de hecho, en autorizaciones en aquellos casos en los que esté claramente permitida la transferencia a un

Fundación Telefónica
Telefónica

tercer país, bien porque el destinatario se encuentre en un país que ofrece una protección adecuada confirmada en una decisión vinculante de la Comisión, bien porque haya suscrito las cláusulas contractuales tipo aprobadas por la Comisión o bien porque el responsable del tratamiento de datos declare que la transferencia se acoge a una de las excepciones previstas en el artículo 26 de la Directiva. Aunque la autoridad de protección de datos puede exigir legítimamente la notificación de dichas transferencias, no es necesario autorizarlas, porque ya están autorizadas por la legislación comunitaria.

La necesidad de buscar un punto intermedio

Una actitud excesivamente laxa en determinados Estados miembros, además de contravenir la Directiva, corre el riesgo de debilitar la protección en el conjunto de la UE, ya que con la libre circulación que garantiza la Directiva es probable que las transferencias internacionales de datos personales se desvíen a los lugares de exportación en los que se impongan menos obligaciones. No obstante, un planteamiento excesivamente estricto impediría respetar las necesidades legítimas del comercio internacional y amenazaría con crear un foso entre la legislación y la práctica, perjudicial para la credibilidad de la Directiva.

Finalmente, debemos señalar que un aspecto a tener muy en cuenta ante una eventual unificación de las normas por medio de la reforma de la Directiva 95/46/CE es el relativo a la determinación de la ley aplicable en materia de protección de datos personales. Un par de cuestiones merecen la atención de la futura reforma:

– Por una parte, la preferencia por el criterio del lugar del establecimiento del responsable del tratamiento de datos. Esta opción persigue beneficiar la actividad internacional de las empresas radicadas en la UE que tratan datos personales. Explicación: todas sus actividades quedan sujetas a una sola ley, que además es la ley del país donde radica el responsable del tratamiento de datos, y además dicha ley regula no solo la responsabilidad civil de la empresa respecto de los particulares, sino también las relaciones administrativas de dicha empresa con las autoridades públicas. Todo ello con independencia de los países donde la empresa responsable ‘trate’ los datos.

– Y por otra parte, el hecho de que la actual Directiva 95/46/CE nada disponga sobre la ley aplicable al tratamiento de datos personales realizado en territorio de terceros Estados sin intervención de medios técnicos en Estados de la UE. Ello explica que la actual Directiva 95/46/CE someta a un régimen muy estricto la circulación de datos personales desde la UE con destino a terceros países.

La apuesta por restaurar la confianza en las transferencias internacionales entre los EEUU y la UE

A finales de septiembre de 2013, *Safe Harbour* contaba con 3.246 empresas adheridas; un aumento muy significativo si lo comparamos con las 400 empresas que había en el año 2004. No obstante, la radiografía actual es inquietante: hay una falta de confianza en las transferencias internacionales de datos entre EEUU y la UE.

Fundación Telefónica
Telefónica

Es el momento de revisar los Principios de Puerto Seguro, aprovechando la reforma de la Directiva 95/46/CE que en estos momentos se está realizando. Se debe pasar a la acción si se quiere mantener la continuidad de los flujos entre los EEUU y la UE: adoptando sin más demoras la reforma de la Directiva 95/46/CE, haciendo seguros los Principios de Puerto Seguro, fortaleciendo las garantías de protección de datos en el área de aplicación de la ley y, en definitiva, promoviendo las normas de protección de datos a nivel internacional.

Razones de seguridad nacional no deben poner en tela de juicio el cumplimiento de los Principios de Puerto Seguro. El funcionamiento de dichos Principios debe seguir basándose en los compromisos y la autocertificación de las empresas que se han adherido. Las empresas tienen que inscribirse mediante notificación al Departamento de Comercio estadounidense, mientras que la Comisión Federal de Comercio de EEUU es responsable de la aplicación de Puerto Seguro.

La inscripción a estas disposiciones es voluntaria, pero las reglas son vinculantes para los que se inscriban. Si una empresa de EEUU quiere adherirse al Puerto Seguro deberá identificar en su política de confidencialidad a disposición del público que se adhiere a los Principios y en realidad cumplir con los mismos, así como autocertificarse.

Los Principios de Puerto Seguro deben seguir actuando como un conducto para la transferencia de los datos personales de los ciudadanos de la UE a EEUU y de las empresas estadounidenses a la UE, en vez de transferirlos a las agencias de inteligencia de EEUU, en virtud de los programas de vigilancia de este país.

En definitiva, el futuro pasa, sin duda alguna, por una revisión de los Principios de Puerto Seguro; por su adaptación a la luz de la experiencia en su aplicación de estos últimos años, poniendo el acento en la protección de datos y no en la seguridad nacional.

Bibliografía recomendada

Aced, E. (2005). Transferencias internacionales de datos. En J. L. Piñar Mañas (Dir.), Protección de datos de carácter personal en Iberoamérica. *II Encuentro Iberoamericano de Protección de Datos, La Antigua- Guatemala, 2-6 de junio de 2003*, pp. 123-125.Valencia: Tirant lo Blanch.

Arribas, J. M. (2002, 7 de marzo). Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EEUU: el sistema de principios de puerto seguro. *La Ley*, No. 5497.

Castañeda, A. (Coord.) (2004). *Derecho tecnológico. Respuestas legales a nuevos retos*. Barcelona: Ediciones Experiencia.

González, L. (2006). El Tribunal de Justicia de las Comunidades Europeas anula el Acuerdo entre la Comunidad Europea y los EEUU para la transmisión de los datos sobre los pasajeros por las compañías aéreas. *Civitas. Revista española de Derecho Europeo*, No. 20, 557-576.

Fundación Telefónica
Telefónica

Hance, O. (1996). Privacy and the Internet: Intrusion, Surveillance and Personal Data. *International Review of Law Computers & Technology*, 10(2), 219-234.

Fundación Telefónica
Telefónica