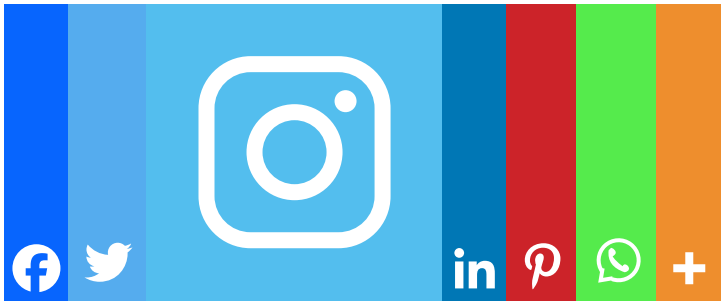
Spread the love



Se comenta en esta entrada un reciente dictamen del Supervisor Europeo de Protección de Datos sobre la Propuesta DORA, con las objeciones formuladas por este supervisor especialmente en el ámbito de la gobernanza interna de datos en las instituciones financieras, de las notificaciones de incidentes a las autoridades y de la trasferencia internacional de datos

El 24 de septiembre de 2020, la Comisión Europea adoptó una Propuesta de Reglamento sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.o 1060/2009, (UE) n.o 648/2012, (UE) n.o 600/2014 y (UE) n.o 909/2014, que ya ha sido objeto de comentarios en este blog (aquí). Como es sabido, esta Propuesta DORA forma parte de un paquete de medidas que incluye también una Propuesta de Reglamento relativo a los mercados de criptoactivos (el «Reglamento MiCA»), una propuesta sobre un régimen piloto de las infraestructuras del mercado basadas en la tecnología de registro descentralizado y una Propuesta para aclarar o modificar determinadas normas conexas de la UE en materia de servicios financieros. Actualmente, la Propuesta DORA está siendo objeto de análisis y debate en el Consejo

Y, en este contexto, el Supervisor Europeo evacuó recientemente un Dictamen preceptivo en el procedimiento prelegislativo correspondiente.,

- En el texto del Dictamen, el SEPD recuerda que cualquier operación de tratamiento de datos, en el contexto de las actividades de las entidades financieras a las que se dirige la Propuesta DORA debe tener como referente los requisitos de protección de datos conforme al RGPD y en particular su artículo 6, como condición básica para asegurar la salvaguardia de los derechos individuales.
    - Con carácter general, ello implica que las entidades financieras deberían **incorporar a su marco de resiliencia operativa digital mecanismos específicos y sólidos de gobernanza de protección de datos.** Ello incluiría sistemas para la determinación de las funciones y las responsabilidades del responsable y del encargado del tratamiento de datos, así como de las actividades de tratamiento que tendrán lugar.
    - Más en particular, considera el SEPD que el sector financiero debe adoptar **códigos de conducta** conformes al art 40

By M.A. Díaz

RGPD en los que se diseñen y delimiten las funciones relativas al tratamiento de datos, así como los procesos de tratamiento justo y transparente

- Dado que en el ámbito de las entidades financieras tienen lugar procesos de almacenamiento de datos, incluidos datos relativos a multas y sanciones, el SEPD recuerda que el **principio de limitación del almacenamiento** requiere que los datos personales se conserven solo durante el tiempo necesario para los fines para los que se hayan recogido. Por ello, y más concretamente, recomienda a las entidades financieras que adopten medidas para garantizar que la **información sobre las multas administrativas se elimine de su sitio web una vez transcurridos cinco años, o antes si ya no es necesaria**. Y, de modo relacionado, en relación con **la publicación de multas administrativas, recomienda incluir entre los criterios que deba valorar la autoridad competente**, los riesgos para la protección de los datos

personales de las personas físicas.

- En cuanto a **la notificación de incidentes graves, el SEPD formula la sugerencia de incluir a las autoridades de protección de datos entre las que directamente reciban estas notificaciones.** Así, el SEPD señala que, en su entender, la redacción del considerando 42 de la Propuesta sería incompatible con el artículo 33 del RGPD. Por ello, recomienda eliminar la referencia a las autoridades de protección de datos del considerando 42 de la Propuesta que las sitúa como receptoras indirectas de las notificaciones, y modificar el artículo 17 para incluir una obligación de notificación directa de vulneraciones de la seguridad de los datos a las autoridades de materia de protección de datos.
    - Este considerando 42, en la redacción inicial de la Comisión Europea establece que: «*Las consecuencias importantes de los ciberataques se amplifican cuando se producen en el sector financiero, un ámbito que corre mucho más riesgo de ser blanco de propagadores malintencionados que persiguen obtener beneficios financieros directamente en la fuente. Para mitigar tales riesgos y evitar que los sistemas de TIC pierdan integridad o dejen de estar disponibles, y que se vulneren datos confidenciales o que las infraestructuras físicas de TIC sufran daños, debe mejorarse significativamente la notificación de incidentes graves relacionados con las TIC por parte de las entidades financieras. La notificación de incidentes relacionados con las TIC debe armonizarse para todas las entidades financieras exigiéndoles que informen únicamente a sus autoridades competentes. Aunque todas las entidades financieras estarían sujetas a esta notificación, no todas ellas deberían verse afectadas de la misma manera, ya que los umbrales de importancia relativa y los plazos pertinentes deben calibrarse para reflejar únicamente los incidentes graves relacionados con las TIC. La notificación directa permitiría a los supervisores financieros acceder a información sobre incidentes relacionados con las TIC. No*

obstante, los supervisores financieros deben transmitir esta información a las autoridades públicas no financieras (autoridades competentes en materia de SRI, ***autoridades nacionales de protección de datos*** *y autoridades policiales o judiciales en caso de incidentes de carácter delictivo). La información sobre incidentes relacionados con las TIC debe canalizarse mutuamente: los supervisores financieros deben proporcionar a la entidad financiera todas las observaciones u orientaciones necesarias, mientras que las AES deben compartir datos anonimizados sobre amenazas y vulnerabilidades relacionadas con un determinado suceso para contribuir a una defensa colectiva más amplia».* Pues bien, frente a esta redacción, el art 33 del RGPD establece la obligación del responsable de tratamiento de notificar a la autoridad de control de datos, en caso de violación de la seguridad de los datos personales, sin dilación indebida y, de ser posible, a 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Añade el art 33 RGPD que si la notificación a la autoridad de control no se efectuase en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos del retraso.

- Por lo que respecta al art 17 de DORA en su redacción inicial, alude a la notificación directa de incidentes, sin contemplar entre las autoridades receptoras de las notificaciones a las de protección de datos, circunstancia que el SEPD sugiere subsanar

- **En relación con las transferencias internacionales a proveedores terceros de servicios de TIC establecidos en un tercer país**, el SEPD recuerda que toda transferencia internacional de datos personales debe cumplir con los requisitos del capítulo V del RGPD con arreglo a su interpretación en la jurisprudencia del TJUE, incluida la sentencia en *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (C-311/18), también conocido simplemente como *Schrems II*. El TJUE declaró es esa sentencia la invalidez de la decisión de adecuación relativa al *Privacy Shield* (escudo de Privacidad) mientras que legitimó las transferencias al

amparo de las cláusulas contractuales tipo (*Standard Contractual Clauses*) aprobadas por la Comisión Europea. Las consideraciones del fallo impactan en las transferencias de datos desde los Estados miembros de la Unión Europea a países fuera del bloque comunitario, incluyendo aquellos en América y, especialmente, a los que no han obtenido una decisión de adecuación.

- Como es sabido, la Unión Europea ha adoptado un sistema de regulación horizontal a través del cual se aprobaron normas generales comprehensivas en materia de protección de datos personales que alcanzan a todas las actividades e industrias. Tal fue el caso de la anterior Directiva 95/46 y su sucesor el RGPD. Estas normas presentan restricciones a las transferencias internacionales de datos a países que no cuenten con normativa considerada adecuada. Por el volumen de relaciones comerciales con Estados Unidos de América resultó necesario tener en cuenta que en este país se carece de una norma general en materia de protección de datos personales, aunque existen regulaciones sectoriales que tratan esta materia y normas de algunos estados que han legislado en materia de privacidad, como es el caso de California. La ausencia de una norma federal ha sido el disparador para que ambos bloques tuvieran que negociar arreglos que permitieran la transmisión de datos. El primero de ellos dio lugar a los principios reconocidos como *Safe Harbor* o Puerto Seguro, adoptados por el Departamento de Comercio de los Estados Unidos, un sistema de autorregulación al cual las empresas en ese país podían adherir, comprometiéndose a respetar ciertas reglas establecidos en su texto. La Comisión Europea declaró adecuado este sistema en el año 2000, mediante su (hoy derogada) Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América
- Sin embargo, pronto se vio que el mecanismo de Puerto Seguro planteaba incongruencias que fueron sancionadas por el TJUE en la relevante sentencia Schrems II.

- Concretamente, el Sr Schrems inició una reclamación contra Facebook Irlanda por considerar que la plataforma social violaba los derechos de intimidad y protección de datos personales de los usuarios. Se basaba el reclamante en que los datos eran transferidos desde Irlanda a servidores localizados en Estados Unidos, en donde eran procesados y utilizados por Facebook Inc. Y, sucedía que en Estados Unidos, los datos podían están sujetos a un control estatal por parte de las agencias de investigación gubernamentales, práctica que podía afectar los derechos de los titulares de datos europeos. En efecto, Facebook Ireland explicó que una gran parte de los datos personales se transfería a Facebook Inc., basándose en cláusulas tipo de protección de datos.
- Schrems cuestionó la compatibilidad del ordenamiento europeo de datos con el Derecho estadounidense que obligaba a la matriz, Facebook Inc., a poner los datos personales recibidos de sus filiales europeas (en este caso de la irlandesa), a disposición de las autoridades estadounidenses, como la *National Security Agency* (NSA) y la *Federal Bureau of Investigation* (FBI) . Y, que esos datos eran utilizados en programas de vigilancia de las autoridades estadounidenses, en modo incompatible con las normas europeas. Por ello, consideró que el ordenamiento europeo no amparaba la transferencia de esos datos a los Estados Unidos y solicitó al regulador de Irlanda que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.
- La autoridad irlandesa de protección de datos inició un procedimiento ante el Tribunal Superior de Irlanda y éste elevó una cuestión prejudicial al Tribunal de Justicia Europeo sobre la interpretación de las disposiciones que validan las transferencias internacionales al amparo de las cláusulas contractuales tipo y el *Safe Harbor*.
- El TJUE **validó las transferencias internacionales al amparo de las cláusulas contractuales tipo**, pero, declaró inválido al *Safe Harbor*. Es decir, consideró que las cláusulas contractuales tipo son una alternativa válida para legitimar la transferencia a países que no posean legislación

adecuada. Sin embargo, en su interpretación estableció que estas cláusulas obligan a las partes a un control activo de la normativa del país de destino, para garantizar que los compromisos asumidos en el contrato no se vean frustrados por las regulaciones del ordenamiento de destino, imposibilitando su cumplimiento. En cambio, sentenció que el *Safe Harbor* no proporciona una adecuada protección y, por lo tanto, no puede ser entendido como un instrumento que avale la transferencia internacional desde la Unión Europea a los Estados Unidos.

- La declaración de invalidez del *Safe Harbor* se basó en dos cuestiones principales. Por una parte que las limitaciones de la protección de datos personales que se derivan de la normativa interna de los Estados Unidos relativa al acceso y la utilización por las autoridades estadounidense de los datos transferidos (principalmente en el marco de investigaciones por las fuerzas de seguridad estatales) no responden a las exigencias en situaciones equivalentes requeridas en el Derecho de la Unión Europea. Además, subrayó el TJUE, en lo que se refiere a la tutela judicial, que los ciudadanos europeos no tienen acceso a los mismos recursos de los que disponen los nacionales estadounidenses contra el tratamiento de datos personales por parte de las autoridades de aquel país. Es por ello que el TJUE resuelve declarar la invalidez del *Safe Harbor* como recurso para las transferencias internacionales.El TJUE declaró inválidas las transferencias internacionales a los Estados Unidos con base en el *Safe Harbor*. Esta anulación derivó en un nuevo mecanismo para legitimar las transferencias internacionales de datos que concluyeron en la aprobación del *Privacy Shield* consensuado por el Departamento de Comercio de los Estados Unidos y las autoridades europeas que dotaba a los ciudadanos europeos de mayores resortes para resguardar sus derechos. En el año 2016 la Comisión Europea declaró válidas las transmisiones de datos certificadas bajo el régimen del *Privacy Shield (Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección*

conferida por el Escudo de la privacidad UE-EE. UU.)

- El *Privacy Shield* se basa en un sistema de autocertificación por el que las entidades estadounidenses se comprometen a cumplir principios de protección de la vida privada —a saber, los principios marco del Escudo de la privacidad UE-EE. UU., incluidos los principios complementarios establecidos por el Departamento de Comercio de Estados Unidos y enumerados en el anexo II de la *Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.*. Se aplica tanto a los responsables como a los encargados del tratamiento. Y los encargados deben estar obligados contractualmente a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la UE y asistirle a responder a las personas físicas que ejerzan sus derechos en caso de transferencia internacional de datos.
- Frente al mecanismo de puerto seguro, el *Privacy Shield* obliga a las entidades responsables de la trasferencia internacional de dato a EEUU a establecer mecanismos de recurso a los particulares afectados por potenciales incumplimientos de modo que los interesados de la UE puedan presentar reclamaciones en relación con el incumplimiento por parte de entidades autocertificadas de EE. UU. Y, a que se resuelvan estas reclamaciones, mediante una resolución que conceda un recurso efectivo

Primavera, by M.A. Díaz

- Finalmente, el SEPD recomienda modificar el artículo 23, apartado 2, de la Propuesta relativo a pruebas avanzadas de las herramientas, los sistemas y los procesos de TIC basadas en pruebas de penetración guiadas por amenazas, para asegurar que no se puedan realizar pruebas, desarrollo de productos o investigaciones de los sistemas de TIC en sistemas de producción activos que contengan datos personales de clientes.

El contenido del Dictamen responde a las competencias que el SEPD tiene atribuidas. Las entidades financieras que quedarán sometidas a DORA en caso de aprobarse, estarán sujetas también al RGPD. Y desde esa perspectiva el Dictamen comentado podría resultar redundante. Sin embargo, no deja de constituir una referencia y una llamada de atención sobre el doble sometimiento, caso de que finalmente las consideraciones contenidas en él no resultasen incorporadas en la Directiva Digital Resilience.