ESCVELA DE PRÁCTiCA JVRíDiCA
SALAMANCA

TRABAJO FIN DE TÍTULO

MÁSTER EN ACCESO A LA ABOGACÍA

Curso 2015/2017

Protección de datos de carácter personal

Manuel Carmelo Martínez Vicente

Marta Civis Valle

Diciembre 2016

TRABAJO FIN DE TÍTULO

MÁSTER EN ACCESO A LA ABOGACÍA

Protección de datos de carácter personal

Personal data protection

Nombre del estudiante: Manuel Carmelo Martínez Vicente
e-mail del estudiante: manuelcarmelo.martinez@outlook.es

Tutor/a: Marta Civis Valle

RESUMEN

El presente trabajo tratará de forma eminentemente práctica la protección de datos de carácter personal, que como consecuencia de la reciente Sentencia el TJUE de 6 de Octubre de 2015, se ha visto en la necesidad de buscar alternativas con respecto a la situación anterior a la misma.

Siendo esta Sentencia el punto de partida que viene a desvirtuar el concepto de Puerto Seguro o Safe Harbor, dicho de forma sencilla, que la transferencia de datos de carácter personal con Estados Unidos y su posterior tratamiento no es seguro para el ciudadano europeo, ya que las autoridades estadounidenses tienen acceso casi indiscriminado a los mismos.

Analizando a fondo dicha sentencia y el marco en el cual se trabajaba antes de ella, haré una comparación de cómo ha quedado configurado el nuevo escenario para la protección de los datos personales y lo que como profesionales del derecho podemos hacer para proporcionar la debida y exigida seguridad en el tránsito y tratamiento de los datos, así como las nuevas posibilidades que van surgiendo para hacer efectiva la protección, las cuales cristalizaron en la Decisión 1250/2016.

PALABRAS CLAVE: Puerto Seguro, Sentencia TJUE 6/10/2015, Decisión 1250/2016, EEUU, seguridad, protección de datos.

ABSTRACT

This work will deal in an eminently practical way with the protection of personal data, which as a consequence of the recent Judgment of the CJEU of October 6, 2015, has been in need of looking for alternatives with regard to the situation prior to it.

This Judgment is the point of departure that is to detract from the concept of Safe Harbor, simply said that the transfer of personal data with the United States and its subsequent treatment is not safe for the European citizen, since The US authorities have almost indiscriminate access to them.

Analyzing in depth this sentence and the framework in which it was worked before it, I will make a comparison of how the new scenario for the protection of personal data has been configured and what, as legal professionals, we can do to provide the due and required security in transit and data processing, as well as the new possibilities that are emerging to make effective the protection, which crystallized in Decision 1250/2016.

KEYWORDS: Safe Harbor, Judgment of the CJEU of October 6, 2015, Decision 1250/2016, USA, security, personal data protection.

Índice

1.- Datos de carácter personal.

1.1.- Importancia y protección.

La Constitución Española establece en el artículo 18 el derecho a la intimidad de las personas:

"18.1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

18.4. La Ley limitará el uso de la Informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.[1]"

El objeto de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[2] la cual derogó a la antigua LORTAD de 1992, es proteger y garantizar, en lo concerniente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas, especialmente con la finalidad de preservar el honor, intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a la posible alteración, pérdida, tratamiento o acceso no autorizado. Todo esto es aplicable a los datos de carácter personal registrados en cualquier tipo de soporte físico susceptible tratamiento ya sea informático o manual.

Los datos de carácter personal según la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, se definen en su artículo 3.a como "cualquier información concerniente a personas físicas identificadas o identificables", quedando también recogida dicha definición en el Reglamento de desarrollo de la misma Ley. Siendo el objeto de la misma "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"[3].

1. Constitución Española, publicada en el BOE núm. 311 de 29 de Diciembre de 1978.

2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

3. Art. 1 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

Como consecuencia de tal definición debemos entender que la Ley cuando habla de datos de carácter personal no solo hace referencia a los que como ciudadanos podamos estar más habituados, que podían ser el nombre y apellidos, sino que como información concerniente se debe entender también otro tipo de información como pueda ser el DNI, fotografías, vídeos, las huellas dactilares, grabaciones de voz, etcétera. Todo ello siempre y cuando los datos hagan referencia a personas físicas identificadas o identificables.

Se han de consideran datos concernientes a personas físicas identificadas, aquellos que sin una posterior averiguación nos dicen de que persona en concreto se trata, este tipo de dato sería el número del DNI, el cual individualiza a la persona y la identifica perfectamente.

Por otro lado, se consideran datos de personas físicas identificables cuando por medio de un cotejo por ejemplo, podemos llegar a averiguar lo que a priori era un desconocido, es decir, tenemos datos suficientes para conocer la identidad de una persona física, situación que se podría dar con las huellas dactilares, que sometidas a tratamiento informático pueden conducir a un sujeto concreto partiendo de un dato de carácter personal. El RD 1720/2007 de desarrollo de la Lopd[4] considera como "persona identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considera identificable si dicha identificación requiere plazos o actividades desproporcionadas[5]".

Para centrar el foco sobre los datos que se consideran incluidos en el concepto de datos de carácter personal y haciendo referencia al formulario que existe en la web de la Agencia Española de Protección de Datos bajo la denominación de "Formulario Nota[6]" se tipifican como datos de carácter personal y más habituales los siguientes:

Datos especialmente protegidos: ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud y vida sexual.

4. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el BOE núm. 17 de 19 de Enero de 2008.

5. Art. 5 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el BOE núm. 17 de 19 de Enero de 2008.

6. Sistema de NOtificaciones Telemáticas a la AEPD (NOTA), aprobado mediante Resolución de la Agencia Española de Protección de Datos de 12 de julio de 2006 publicado en el BOE núm. 181 de 31 de julio de 2006.

Datos de carácter identificativo: DNI/NIF, dirección, imagen, voz, número de la seguridad social, marcas físicas, teléfono, firma, huellas, nombre, apellidos, firma electrónica, tarjeta sanitaria.

Datos relativos a las características personales: datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.

Datos relativos a las circunstancias sociales: alojamiento, vivienda, situación familiar, propiedades, posesiones, aficiones, estilos de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.

Datos académicos y profesionales: formación, titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales.

Datos de empleo: profesión, puestos de trabajo, datos no económicos de la nómina, historial del trabajador.

Datos que aportan información comercial: actividades y negocios, licencias comerciales, subscripciones a publicaciones o medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.

Datos económicos, financieros y de seguros: ingresos, rentas, inversiones, bienes patrimoniales, créditos, avales, préstamos, planes de pensiones, datos bancarios, datos económicos de la nómina, datos hipotecas, subsidios, deducciones impositivas, impuestos, seguros, historial de créditos, tarjetas de crédito.

Datos relativos a transacciones de bienes y servicios: bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el mismo, transacciones financieras, compensaciones, indemnizaciones.

Estos datos han de ser recogidos con el consentimiento de su titular, siendo este consentimiento fundamental en la protección de datos. Dicho consentimiento debe ser prestado con anterioridad a facilitar los datos al Responsable del Fichero para que proceda a su tratamiento, garantizando así que el titular conoce tanto la finalidad, como sus derechos, así como los datos del Responsable del Fichero que deberán ser proporcionados al interesado en ese momento. La regla general que establece la LOPD es la de solicitar a los titulares de los datos el "consentimiento, libre, específico, informado e inequívoco[7]". Concretamente, cada uno de estos requisitos implica:

7. Art. 3 h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

Libre, deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos que se establecen en el Código Civil.

Específico, es decir, referido a una operación de tratamiento y una finalidad determinadas, explícitas y legítimas del Responsable del Tratamiento, tal y como se establece en el artículo 4.2 de la Ley Orgánica 15/1999.

Informado, es decir, que el afectado conozca con anterioridad al tratamiento la existencia del fichero y las finalidades para las que se lleva a cabo su tratamiento. Es por ello que el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de puntos que en el fichero se contienen.

Inequívoco, lo que implica que no resultará admisible la deducción del consentimiento proveniente de los meros actos realizados por el afectado, lo que se conoce como consentimiento presunto, siendo preciso que existan una acción u omisión expresas que impliquen la existencia de ese consentimiento.

Por consiguiente y como profesionales del derecho y quedando también orientado a nuestros futuros clientes, nunca nos podrán solicitar el consentimiento para tratar nuestros datos personales, de forma que no conozcamos la finalidad para que son tratados, cuál es la forma de ejercicio de nuestros derechos, y quién es en última instancia el Responsable del Fichero sin que todo ello se derive claramente de nuestros actos, quedando claro que deseábamos prestar el consentimiento.

Otra de las características principales del consentimiento y que debe cumplirse según lo dispuesto en el art. 6 de la LOPD es "salvo disposición en contrario" es el hecho de que la aceptación por parte del afectado debe ser inequívoca, expresa o tácita, siendo obligatoria tanto para la aceptación expresa como para la aceptación tácita que sea inequívoca.

No obstante para que el consentimiento tácito vaya a ser considerado inequívoco, será preciso dar al afectado un plazo prudencial, para que dentro del mismo, pueda tener conocimiento de que con su omisión de oponerse al tratamiento, lo que implica es un consentimiento al mismo. Dependiendo del tipo de datos que se estén solicitando, el tipo de consentimiento puede variar, como hemos dicho antes hay datos que solo se puede recabar con el consentimiento expreso de su titular.

A continuación se indican una serie de datos personales respecto a los que el consentimiento debe cumplir una serie de características especiales[8]:

8. Art. 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

Consentimiento expreso y por escrito: En caso de que los datos solicitados sean relativos a la ideología, afiliación sindical, religión y creencias.

Consentimiento expreso: Los datos de carácter personal relativos al origen racial, a la salud y a la vida sexual exclusivamente podrán ser tratados, cedidos y recabados cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

No obstante, existen excepciones relativas a la prestación del consentimiento. Exclusivamente podrán recabarse datos personales sin mediar consentimiento en caso de que:

Sean datos recabados por las Administraciones Públicas para el ejercicio de sus funciones y dentro de sus competencias. Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado (tales como la vida o la integridad física).

Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el Responsable del Fichero o por el tercero a quien se comuniquen los datos.

Una vez que conocemos los datos que son relevantes, debemos señalar las obligaciones legales básicas que marca la normativa de protección de datos:

Calidad de los datos: los datos de carácter personal se podrán recoger para su tratamiento siempre que sean adecuados, pertinentes y no excesivos en relación con el ámbito en el que se encuadran y las finalidades para que se recogen determinadas, explícitas y legítimas, no podrán usarse para otras finalidades incompatibles con aquellas, serán exactos y se han de poner al día de forma que respondan con veracidad a la situación actual del afectado y habrán de ser cancelados cuando hayan dejado de ser necesarios o pertinentes (Art. 4 LOPD[9]).

9. Art. 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

Deber de secreto: están obligados al secreto profesional tanto el Responsable del Fichero y como quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal y al deber de guardarlos, estas obligaciones subsistirán después de finalizar las relaciones con el titular de los ficheros (Art. 10 LOPD[10]).

Información en la recogida de los datos de carácter personal: los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del tratamiento. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos estas advertencias en forma claramente legible (Art. 5 LOPD[11]).

10. Art. 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

11. Art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

Sin embargo, estos tipos de datos sí podrán tratarse cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario o equivalente, sujeto al secreto profesional (Art. 7 LOPD[12]). Sin perjuicio de lo que se dispone en el artículo 11 de la LOPD respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad (Art. 8 LOPD[13]).

Comunicación o cesión de datos: Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado. Sin embargo este consentimiento no será preciso cuando la cesión esté autorizada en una Ley, o cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica (cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros), o cuando los datos procedan de fuentes accesibles al público, o cuando la cesión sea de datos relativos a la salud y sea necesaria para solucionar una urgencia (que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica), o cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos (Art. 11 LOPD[14]).

12. Art. 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

13. Art. 8 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

14. Art. 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

Tratamiento por cuenta de terceros: Deberá estar regulado en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el Encargado del Tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad del RD 1720/2007[15] que el encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del fichero, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Inscripción de los ficheros en el Registro General de la Agencia Española de Protección de Datos (RGPD): en el caso de ficheros de titularidad pública con la previa publicación en Boletín Oficial de una Disposición General con la declaración de los ficheros (Artículos 20, 25 y 26 LOPD, y Título V del R.D. 1720/2007).

Tutela del derecho de los afectados de acceso, rectificación y cancelación: estableciendo el procedimiento interno apropiado (Artículos 15 a 17 LOPD, y Título III del R.D. 1720/2007).

Redacción e implantación del documento de seguridad: que incluya toda la normativa de seguridad de índole técnica y organizativa necesaria para garantizar la seguridad de los datos objeto de tratamiento. Será de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información (Art. 9 LOPD y Título VIII, capítulo II, del RD 1720/2007).

15. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el BOE núm. 17 de 19 de Enero de 2008.

Una vez que hemos demarcado los conceptos básicos, vamos a centrar el tema de este trabajo, la transferencia internacional de estos datos de carácter personal, el artículo 5.1 s) del Reglamento de desarrollo de la Ley Orgánica 15/1999[16] nos define la Transferencia internacional de datos como el "Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".

Siendo este tipo de tratamiento de los datos los que más problemas han causado como veremos más adelante, ya que entran en conflicto distintas regulaciones, más concretamente me centraré en la problemática de la transferencia de datos con Estados Unidos, siendo este país el receptor y Europa el lugar donde residen los ciudadanos, nuestros posibles clientes, y cómo podemos dar una solución factible a los problemas que se nos pueden plantear tanto de manera profesional como en el ámbito más personal con nuestros propios datos, ya que cada vez más usamos plataformas para la transferencia como Google docs, Google drive, Dropbox y veremos casos prácticos relacionados con estos sistemas de almacenamiento y transferencia de datos en la nube.

16. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el BOE núm. 17 de 19 de Enero de 2008.

1.2.- Visión práctica de la importancia y la protección de los datos de carácter personal.

Como letrados, hemos de ser capaces de tener una visión global y práctica de lo que significa la protección de los datos de carácter personal, hecho que se pierde muchas veces por etéreo o por desactualización de conocimientos, ya que el campo de la protección de estos datos va íntimamente ligada a la informática.

Pues bien, la jurisprudencia por medio de sentencias de los diferentes estratos jurisdiccionales, tanto nacionales como internacionales, se ha ido encargando de enmarcar y afinar cada vez más el contenido y la importancia de la protección de estos datos.

La Sentencia del TJUE de 8 de abril de 2014 Caso "Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources[17]", recoge dentro de su marco jurídico la Directiva 95/46/CE[18], que dice textualmente en su artículo 17 " Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse."

17. http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=ES Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014. Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung (C-594/12) y otros.

18. Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (ConsejoDeEuropa, 1995)

Como se desprende del mismo artículo, son los Estados los garantes últimos de la protección, siendo ellos los responsables de modular dicha protección, como se recoge en la STEDH 2014/34 de 27 de mayo de 2014, Caso De La Flor Cabrera contra España[19]. "La elección de medidas propias para garantizar el cumplimiento del artículo 8 del Convenio en los informes interindividuales depende en principio del margen de valoración de los Estados Contratantes, sean las obligaciones a cargo del Estado positivas o negativas. En efecto, existen varias maneras diferentes de asegurar el respeto de la vida privada.

En este sentido, en asuntos relativos a la divulgación de datos de carácter personal, el Tribunal ha reconocido que convendría conceder a las autoridades nacionales competentes cierta libertad para establecer un equilibrio justo entre los intereses públicos y privados que se encuentren en juego. Sin embargo, este margen de valoración va a la par con un control europeo (Funke contra Francia, Sentencia de 25 febrero 1993, serie A núm. 256-A, ap. 55[20]) y su alcance va en función de factores como la naturaleza y la importancia de los intereses en juego y la gravedad de la injerencia (Z contra Finlandia, Sentencia de 25 febrero 1997 [TEDH 1997, 13] , Repertorio de sentencias y decisiones 1997-I, pg. 348, ap. 99[21])."

19.http://www.mjusticia.gob.es/cs/Satellite/Portal/1292427055095?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DSentencia_DE_LA_FLOR_CABRERA_c._Espa%C3%B1a.pdf&blobheadervalue2=Docs_TEDH Espa%C3%B1a.pdf&blobheadervalue2=Docs_TEDH

20.http://hudoc.echr.coe.int/eng#{"fulltext":["funkeof france"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57809"]}

21.http://hudoc.echr.coe.int/eng#{"fulltext":["finlande25fevrier1997"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-62593"]}

Si bien en el caso que atañe a la sentencia recaída el 8 de abril de 2014 Caso Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources, lo que se dilucida es la obligación de una compañía de telefonía de conservar los datos y el acceso que puede tener un Estado a los mismo en base a una investigación terrorista, pero si bien es cierto "Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan."[22]

Por lo que como abogados, debemos tener en cuenta que de unos datos considerados que aislados y sin el tratamiento oportuno, no tienen aparente relevancia, en su conjunto puedan acarrear consecuencias para un cliente, tales como ubicar su situación en un momento concreto, el recorrido que realizó hasta ese punto o dónde se desplazó después. Sin embargo también puede tener una vertiente positiva a la hora de confirmar una coartada o realizar un patrón de comportamiento de nuestro cliente y desmontar teorías de la contraparte con datos objetivos.

Es importante su protección porque como dice la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (LCEur 1995, 2977) , relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), tiene por objeto, conforme a su artículo 1, apartado 1, "garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas en lo que respecta al tratamiento de los datos personales"[23].

22. http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=ES Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014. Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung (C-594/12) y otros.

23. Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Estamos hablando entonces de la protección de derechos fundamentales recogidos en legislación supranacional y como que como recuerda el TEDH en su sentencia 2014/34 de 27 de mayo de 2014, Caso De La Flor Cabrera[24] contra España pertenecen a la vida privada del individuo "El Tribunal recuerda que la noción de «vida privada» es una noción amplia, no susceptible de una definición exhaustiva, que cubre la integridad física y moral de la persona y, por tanto, engloba múltiples aspectos de la identidad de un individuo, tales como el nombre o los elementos que hacen referencia al derecho de imagen (Von Hannover contra Alemania, núm. 2, núms. 40660/2008[25]. Esta noción comprende las informaciones personales que un individuo puede legítimamente esperar que no sean publicadas sin su consentimiento". Y como profesionales debemos tener especial atención a este tipo de circunstancias que muchas veces se escapan del alcance de la legislación española y hemos de acudir a normas de carácter europeo para la defensa de la protección de datos dentro de la jurisdicción española.

24.http://www.mjusticia.gob.es/cs/Satellite/Portal/1292427055095?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DSentencia_DE_LA_FLOR_CABRERA_c._Espa%C3%B1a.pdf&blobheadervalue2=Docs_TEDH Espa%C3%B1a.pdf&blobheadervalue2=Docs_TEDH

25. STEDH Estrasburgo (Sección 3ª) de 24 junio 2004. TEDH 2004\45. Jurisdicción: Protección Europea de Derechos Humanos. Demanda núm. 59320/2000. Asunto Von Hannover contra Alemania.

http://www.sbdp.org.br/arquivos/material/1706_ASE_OF_VON_HANNOVER_v._GERMANY_No._2_Spanish_Translation_by_the_COEECHR_and_Thomson_Reuters_Aranzad.pdf.

Tal es la importancia práctica de estos datos que se llegó a "Declarar contrario a la Constitución y nulo el inciso «cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o» del apartado 1 del art. 21 de la Ley Orgánica 15/1999, de 13 de diciembre (RCL 1999, 3058) , de Protección de Datos de Carácter Personal[26].

Declarar contrarios a la Constitución y nulos los incisos «impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas» y «o administrativas» del apartado 1 del art. 24, y todo su apartado 2, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."[27] En la Sentencia del Tribunal Constitucional núm. 292/2000 de 30 noviembre. RTC 2000\292, en cuyos fundamentos jurídicos se recogen las siguientes manifestaciones: "Pese a la importancia que para garantizar el ejercicio del derecho fundamental poseen los derechos del interesado a ser informado y a consentir la cesión de sus datos personales, como antes se ha declarado, sin embargo, es suficiente según el art. 21.1 LOPD que la comunicación de tales datos entre Administraciones Públicas, para el ejercicio de competencias diferentes o que versen sobre materias distintas, sea autorizada por una norma reglamentaria. Al respecto, ya hemos dicho [STC 127/1994 (RTC 1994, 127) , F. 5, con remisión a la STC 83/1984, F. 4, y 99/1987 (RTC 1987, 99) , F. 3 a)] que incluso en los ámbitos reservados por la Constitución a la regulación por Ley no es imposible una intervención auxiliar o complementaria del Reglamento, pero siempre que estas remisiones restrinjan efectivamente el ejercicio de esa potestad reglamentaria a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley. De tal modo que esa remisión no conlleve una renuncia del legislador a su facultad para establecer los límites a los derechos fundamentales, transfiriendo esta facultad al titular de la potestad reglamentaria, sin fijar ni siquiera cuáles son los objetivos que la reglamentación ha de perseguir, pues, en tal caso, el legislador no haría sino «deferir a la normación del Gobierno el objeto mismo reservado» (STC 227/1993, de 9 de julio [RTC 1993, 227] , F. 4, recogiendo la expresión de la STC 77/1985, de 27 de junio [RTC 1985, 77] , F. 14)".[28]

26. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

27. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

28. https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

La remisión a la regulación reglamentaria de materia ligada a la reservada a la Ley es preciso, pues, que se formule en condiciones tales que no contraríe materialmente la finalidad de la reserva, de la cual se derivan, según la STC 83/1984, «ciertas exigencias en cuanto al alcance de las remisiones o habilitaciones legales a la potestad reglamentaria, que pueden resumirse en el criterio de que las mismas sean tales que restrinjan efectivamente el ejercicio de esa potestad a un complemento de la regulación legal que sea indispensable por motivos técnicos o para optimizar el cumplimiento de las finalidades propuestas por la Constitución o por la propia Ley»[29]. Es en este segundo plano en el que se encuentra el núcleo argumental del recurso interpuesto por el Defensor del Pueblo que es acogido en esta Sentencia, el cual considera que al establecer el art. 21.4 LOPD que esas cesiones no requieren del previo consentimiento del afectado permite al reglamento imponer un límite al derecho fundamental a la protección de datos personales, que como se ha dicho ya, defrauda la previsión del art. 53.1 de la Constitución (STC 101/1991, de 13 de mayo [RTC 1991, 101] , F. 3)[30].

El motivo de la inconstitucionalidad del art. 21.1 LOPD resulta, pues, claro. La LOPD en este punto no ha fijado por sí misma, como le impone la Constitución en el art. 53.1, los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado [art. 11 LOPD, en relación con lo dispuesto en los arts. 4, 6 y 34 e) LOPD], sino que se ha limitado a identificar la norma que puede hacerlo en su lugar. Norma que bien puede ser reglamentaria, ya que con arreglo al precepto impugnado será una norma de superior rango, y con mayor razón para el caso de que la modificación lo sea por una norma de similar rango, a la que crea el fichero (y ésta basta con que sea una disposición general, que no una Ley, publicada en un Boletín o Diario oficial –art. 20.1 LOPD–) la que pueda autorizar esa cesión inconsentida de datos personales, lo que resulta ser, desde luego, contrario a la Constitución."[31]

29. http://www.congreso.es/constitucion/ficheros/sentencias/stc_083_1984.pdf

30. https://www.boe.es/diario_boe/txt.php?id=BOE-T-1991-15519

31. LESMES SERRANO, C., BAISÁN GARCÍA, N., FERNÁNDEZ GARCÍA J. A., GUERRERO ZAPLANA, J. y otros. *Ley de Protección de datos. Análisis y comentario de su jurisprudencia*. (2008). España. Ed. LEX NOVA.

2.- El escenario de la protección de datos de carácter personal

Vivimos en una sociedad en constante cambio y en lo que se refiere a la protección de datos, es una materia íntimamente ligada a la informática, por lo que supone un cambio casi a diario, haciendo muchas veces que sea difícil llegar a conocer un asunto en profundidad por la futilidad de las leyes en las que se basa o por los constantes cambios que puede sufrir el mismo asunto en sí.

Todo esto sin mencionar los cambios drásticos que pueden suponer las resoluciones judiciales tanto nacionales como internacionales, siendo esto último nuestro caso, con la STJUE de 6 de octubre de 2015, se han desmontado creencias que se consideraban consolidadas y que ofrecían al ciudadano una protección adecuada en lo que se refiere a sus datos de carácter personal. Para conocer desde una posición práctica lo que ha ocurrido, haremos un repaso por la situación anterior a la sentencia y los cambios que ha introducido con respecto a la protección de datos de carácter personal.

Antes de llegar la mencionada sentencia tenemos que ser consciente de dónde viene el concepto de Puerto Seguro, en 1999 los Estados Unidos iniciaron negociaciones con la Unión Europea para conseguir una declaración de adecuación del nivel de protección de datos personales. El problema inicial era que en los Estados Unidos no existe, dado el marcado carácter autorregulador del comercio, una normativa sobre protección de datos de carácter personal aplicable en todo el territorio y en todos los sectores de actividad.

A fin de superar los problemas derivados de esta dispersión normativa, el Departamento de Comercio de los Estados Unidos presentó, como documento para la discusión entre las autoridades norteamericanas y de la Unión Europea un borrador de "principios de puerto seguro", a fin de garantizar a los operadores que se adhirieran a los mismos una "presunción de adecuación" al nivel de protección exigido por la UE, permitiéndose así la libre transferencia internacional de datos a dichos operadores. Para ello, aquéllos debían manifestar ante la Oficina Federal de Comercio (u otra entidad por ella designada) su adhesión a estos principios y su compromiso de llevarlos a la práctica, adoptando para ello las medidas adecuadas.[32]

32.https://www.agpd.es/portalwebAGPD/internacional/adecuacion/estados_unidos/common/pdfs/ElAcuerdodePuertoSeguroconlosEstadosUnidos.pdf

El Acuerdo de Puerto Seguro consta de siete principios básicos, que adelante desarrollaré, referidos a la notificación, opción, transferencia ulterior a terceras empresas, seguridad, integridad de los datos, derecho de acceso y aplicación. Dichos principios son, como se indicó, complementados con las "preguntas más frecuentes", básicamente referidas a tipos específicos de datos o tratamientos.

La Comisión Europea, mediante su Decisión de 26 de Julio de 2000, y con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, se pronunció sobre la adecuación 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.

2.1.- Situación anterior a la STJUE de 6 de octubre de 2015.

Desde hace algo más de 15 años se venía contemplando una situación estable en lo que se refiere al marco de protección de los datos de carácter personal, todo ello derivado de normas supranacionales como son las Directivas y Decisiones de los distintos órganos de la Unión Europea, siendo las más relevantes para este asunto la Directiva 95/46/CE[33] y la Decisión 2000/520/CE[34], quedando ligadas y haciendo referencia una a la otra.

La Decisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, vino a definir el puerto seguro, lo que se consideraría como una seña de seguridad en la transferencia internacional de datos de carácter personal. Este hito se compone de diferentes principios que quedan recogidos en el Anexo I de la Decisión[35] y que son fruto de las negociaciones mantenidas entre la Unión Europea y Estados Unidos.

33. https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

34. https://www.boe.es/buscar/doc.php?id=BOE-A-2000-22726

35.http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

PRINCIPIOS DE PUERTO SEGURO[36]

NOTIFICACIÓN. Las entidades informarán a los particulares de los fines con los que cuales recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales la información se revelará; las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación. La notificación se hará en lenguaje claro y transparente la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero.

ELECCIÓN. Las entidades ofrecerán a los particulares la posibilidad de decidir (exclusión) si su información personal: puede divulgarse a un tercero o bien puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular. Se deben proporcionar a los particulares mecanismos claros y transparentes, fácilmente disponibles y asequibles para ejercer su derecho de opción. Si se trata de información delicada, como datos sobre el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical o la vida sexual de la persona, la opción de participar será afirmativa o explícita si la información va a revelarse a un tercero o a utilizarse para un fin distinto del que inicialmente motivó la recogida de información o de una manera distinta a la autorizada con posterioridad por éste al optar por la «aceptación». En cualquier caso, una entidad debe tratar como delicada toda información recibida de un tercero cuando dicho tercero la identifique y la trate como información delicada.

TRANSFERENCIA ULTERIOR. Para revelar información a terceros, las entidades deberán aplicar los principios de notificación y opción. Cuando una entidad desee transferir los datos a un tercero que actúe como agente, como se describe en la nota final, podrá hacerlo si previamente se asegura de que éste suscribe los principios, si es objeto de una resolución sobre su «adecuación» con arreglo a la Directiva u otra disposición o si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios.

36. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478256785205&uri=CELEX:32000D0520

Si la entidad cumple estos requisitos, no será responsable (a menos que la propia entidad acuerde lo contrario) del tratamiento realizado por el tercero a quien haya transferido este tipo de información y que vulnere las limitaciones o estipulaciones establecidas, a menos que la entidad sepa, o debiera saber, que el tercero realizaría dicho tratamiento y no haya adoptado medidas razonables para impedir o detener tal tratamiento.

SEGURIDAD. Las entidades que creen, mantengan, utilicen o difundan información personal tomarán precauciones razonables para evitar su pérdida, su mal uso y consulta no autorizada, su divulgación, su modificación y su destrucción.

INTEGRIDAD DE LOS DATOS. De acuerdo con los principios, la información personal debe ser pertinente para los fines con los que se utiliza. Una entidad no podrá tratar la información personal de manera incompatible con los fines que motivaron su recogida o aprobó posteriormente el particular. En la medida necesaria para alcanzar dichos fines, las entidades adoptarán medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales.

ACCESO. Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona; o cuando puedan vulnerarse los derechos de otras personas.

APLICACIÓN. Una protección eficaz de la vida privada debe incluir mecanismos para garantizar la conformidad con los principios, una vía de recurso para las personas a que se refieran los datos y se vean afectadas por el incumplimiento de dichos principios y sanciones contra la entidad incumplidora. Como mínimo, tales mecanismos deben incluir: a) una vía de recurso independiente, asequible e inmediatamente disponible para investigar y resolver con arreglo a los principios las denuncias y litigios de los particulares y otorgar daños y perjuicios donde determinen la legislación aplicable o las iniciativas del sector privado; b) procedimientos de seguimiento para comprobar que los certificados y declaraciones de las empresas sobre sus prácticas en materia de vida privada se ajustan a la verdad y que dichas prácticas se aplican en consecuencia; y c) obligación de subsanar los problemas derivados del incumplimiento de los principios para las entidades que se hayan adherido a ellos y las sanciones correspondientes contra ellas, que serán lo suficientemente rigurosas para garantizar su cumplimiento.

Publicados en un primer momento por el Departamento de Comercio de Estados Unidos de América el 21 de julio de 2000, se incorporaron también a la Decisión.

Una vez que entró en vigor la legislación general sobre la protección de la vida privada en la Unión Europea, es decir, la Directiva relativa a la protección de datos, sólo pueden transferirse datos personales a aquellos países no comunitarios que ofrezcan un nivel adecuado de protección de la vida privada.

Según la Agencia Española de Protección de Datos[37], un nivel de protección adecuado será otorgado a un país cuando cumpla procedimiento de autorización de Transferencias Internacionales de Datos:

La autorización de transferencias internacionales de datos se tramitará en el Registro General de Protección de Datos conforme al procedimiento establecido en la sección primera del capítulo V del título IX del RLOPD[38].

El procedimiento se inicia a solicitud del exportador que pretenda llevar a cabo la transferencia.

En su caso, se podrá requerir al solicitante para que complete o modifique la documentación presentada en el plazo de 10 días, establecido en el artículo 71.1 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común. Si transcurrido dicho plazo no se hubiera recibido su notificación, se le tendrá por desistido de su petición, procediéndose al archivo de su solicitud. El trámite de información pública con carácter potestativo es de 10 días.

Cumplidos los requisitos legalmente exigibles, la Directora de la Agencia resolverá autorizar la transferencia internacional de datos, y se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

37. http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

38. http://boe.es/diario_boe/txt.php?id=BOE-A-2008-979

El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Constituye infracción muy grave, de acuerdo con lo dispuesto en el artículo 44.4.d) de la LOPD, "La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria".

Por otra parte, la AGPD en aquéllos supuestos en los que sea necesaria la autorización de la Directora de la Agencia Española de Protección de Datos para transmisiones de datos fuera del territorio del EEE, podrá otorgar la autorización en caso de que, además de observarse lo que establece la LOPD, el exportador aporte las garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

De conformidad con lo dispuesto en el artículo 33 de la LOPD, la autorización de transferencia internacional de datos a un país que no ha sido declarado como país con un nivel adecuado de protección sólo podrá otorgarse si se obtienen garantías suficientes. Así, podrá ser otorgada si el responsable del fichero aporta un contrato escrito, celebrado entre el exportador y el importador de datos, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

Transferencias Internacionales de datos entre responsables de tratamiento.

Para este tipo de transferencias se considerarán que reúnen las garantías adecuadas los contratos celebrados en los términos previstos en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001[39], y 2004/915/CE, de 27 de diciembre de 2004[40], por la que se modifica la anterior.

39.https://www.boe.es/doue/2001/181/L00019-00031.pdf

40.https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/Dec_2004_915_CE_271204_vers_consoli.pdf

Cada una de las Decisiones de la Comisión Europea contiene un conjunto de cláusulas contractuales tipo. Los responsables del tratamiento podrán optar por uno u otro conjunto de cláusulas, pero no podrán modificarlas ni combinar elementos de distintas cláusulas ni de los conjuntos.

Transferencias Internacionales de datos de responsable a encargado del tratamiento.

Cuando la transferencia de datos se realice entre un responsable y un encargado del tratamiento se considerarán que reúnen las garantías adecuadas los contratos que incluyan las cláusulas contractuales tipo establecidas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010[41].

Se entiende según el glosario de la AGPD[42] como responsable del fichero o del tratamiento: "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente."

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará responsable del tratamiento a la persona o personas integrantes de los mismos.

Y se define a encargado del tratamiento como: "la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio."[43]

En el caso de entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados, se considerará encargado del tratamiento a la persona o personas integrantes de los mismos.

41. http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32010D0087

42.https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php

43.https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php

Se podrán autorizar transferencias internacionales de datos entre un encargado del tratamiento/exportador de datos, establecido en España, y un subencargado del tratamiento/importador de datos, ubicado en un país que no garantiza un nivel adecuado de protección, siempre que por el exportador de datos se aporten las garantías suficientes de respeto a la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

Se considerará que proporcionan las garantías adecuadas los contratos que incluyan las cláusulas tipo adoptadas por la Agencia Española de Protección de Datos en su resolución de Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012.

Además del contrato entre el encargado del tratamiento/exportador de los datos e importador/subencargado del tratamiento, se requiere el contrato marco entre el responsable del tratamiento y el encargado del tratamiento/exportador de datos en el que aquél autorice la subcontratación y la transferencia internacional de datos.

Pero además hay supuestos legalmente excepcionados de la autorización de la Directora de la Agencia Española de Protección de Datos[44]:

El artículo 34 de la LOPD y 66.2 del RLOPD establecen los supuestos en los que no será necesaria la autorización previa de la Directora de la Agencia Española de Protección de Datos:

Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.

Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional

Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.

44.https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides idphp.php

Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

Por consiguiente, hay unos países que tienen acordado un nivel adecuado de seguridad para la transferencia y tratamiento de datos de carácter personal, hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes[45]:

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

Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003

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

45.https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

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

Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016., que posteriormente analizaremos. En la página web del Escudo de privacidad se accede a la relación de las entidades certificadas: https://www.privacyshield.gov/list

Debe recordarse que en el caso de que la transferencia internacional de datos con destino a uno de estos países sea consecuencia de una prestación de servicios, esta circunstancia no exime de la obligación de tener que suscribir un contrato conforme a lo dispuesto en el artículo 12 de la LOPD[46].

Aunque Estados Unidos de América y la Unión Europea comparten el objetivo de mejorar la protección de la vida privada de sus ciudadanos, los primeros siguen un enfoque diferente al de la Unión Europea. El planteamiento de Estados Unidos es sectorial y tiene como fundamento una mezcla de legislación, reglamentación, y autorregulación. Dadas las diferencias, muchas entidades estadounidenses han expresado su inquietud sobre las consecuencias del nivel de adecuación que exige la Unión Europea para las transferencias de datos personales desde la Unión Europea a Estados Unidos de América.

46. Art. 12 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el BOE núm. 298 de 14 de Diciembre de 1999.

2.2.- Situación que deriva en la Sentencia del TJUE de 6 de octubre de 2015.

Todo se remonta a 2013, cuando en junio, Edward Joseph Snowden[47] que fue consultor tecnológico, informante y antiguo empleado de la CIA[48] (Agencia Central de Inteligencia) y de la NSA[49] (Agencia de Seguridad Nacional) hizo públicos, a través de los periódicos The Guardian[50] y The Washington Post[51], documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM[52] y XKeyscore[53]. El Washington Post informó que el motivo de las filtraciones era destapar el «Estado de vigilancia» existente en Estados Unidos.

Para justificar la filtración, Snowden comentó que no puede "en conciencia, permitir al gobierno de Estados Unidos destruir la privacidad, la libertad en internet y las libertades básicas de la gente de todo el mundo con esta gigantesca máquina de vigilancia que están construyendo en secreto". No quiero vivir en una sociedad que hace este tipo de cosas… No quiero vivir en un mundo donde se registra todo lo que hago y digo. Es algo que no estoy dispuesto a apoyar o admitir". (Edward Snowden, hablando con The Guardian, en junio de 2013)[54]

47.http://cnnespanol.cnn.com/2013/06/10/quien-es-edward-snowden-el-hombre-que-filtro-datos-secretos-de-la-nsa/

48. https://www.cia.gov/es

49. https://www.nsa.gov

50. https://www.theguardian.com/international

51. https://www.washingtonpost.com/

52. https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

53. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

54. http://internacional.elpais.com/internacional/2013/06/10/actualidad/1370865085_661307.html

Uno de los programas que destapó Snowden fue PRISM. Este es el nombre que recibe un programa clandestino de vigilancia electrónica operado por la Agencia de Seguridad Nacional de los Estados Unidos para la recogida masiva de comunicaciones procedentes de al menos nueve grandes compañías estadounidenses de Internet.

Este programa secreto, filtrado a la opinión pública en 2013, fue puesto en marcha en 2007, en el marco de la expansión de los servicios de inteligencia de Estados Unidos iniciada en 2001 tras los atentados del 11 de septiembre.

PRISM es el nombre en clave utilizado por el gobierno estadounidense en su esfuerzo por recopilar datos, conocido oficialmente como «SIGAD US-984XN». PRISM recoge y almacena las comunicaciones de Internet a partir de las demandas que la NSA emite a las empresas de Internet, como Google, amparándose en la Ley de enmiendas a FISA[55] de 2008, para que las compañías entreguen todos los datos que coincidan con los términos de búsqueda aprobados por el tribunal FISA.

La NSA puede utilizar estas solicitudes para hacerse con las comunicaciones cifradas durante su viaje por el backbone[56] de Internet y así centrarse en los datos almacenados que los sistemas de telecomunicaciones previamente han filtrado y descartado, y así obtener datos más fáciles de manejar, entre otras ventajas.

PRISM se inició en 2007 gracias a la aprobación de la Protect America Act[57] por el gobierno de George W. Bush[58]. El programa operó bajo la supervisión del Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos[59], conforme a la Ley de Vigilancia de la Inteligencia Extranjera (FISA)[60].

La existencia de PRISM se filtró seis años más tarde gracias a Edward Snowden, quien advirtió que el alcance de la recopilación masiva de datos era mucho mayor de lo que la población conocía. Las revelaciones empezaron a ser publicadas por The Guardian y The Washington Post el 6 de junio de 2013.

55. Foreign Intelligence Surveillance Act of 1978 (FISA) Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. cap. 36

56. http://backbonejs.org/

57. https://www.justice.gov/archive/ll/

58. http://www.biografiasyvidas.com/biografia/b/bush_george.htm

59. http://www.fisc.uscourts.gov/

60. Foreign Intelligence Surveillance Act of 1978 (FISA) Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. cap. 36

Los documentos posteriormente publicados demostraron los acuerdos financieros que existían entre la Special Source Operations[61], la división de la NSA responsable de PRISM, y las empresas estadounidenses de las que se extraían datos, que entregaban los datos a cambio de millones de dólares.

Los documentos indican que PRISM es «la fuente número uno de la inteligencia primaria utilizada para los informes analíticos de la NSA» y a través del cual la agencia ha obtenido el 91% del tráfico de Internet interceptado bajo la FISA section 702 authority[62]. La información filtrada se publicó un día después de que se revelase que el Tribunal de FISA[63] había obligado a una subsidiaria de la empresa de telecomunicaciones Verizon[64] a entregar los registros de seguimiento de todas las llamadas telefónicas de sus clientes a la NSA.

Pues bien, una vez conocidas estas revelaciones y como la NSA conocía datos privados de la población que no debieran estar en su poder, el austriaco Maximillian Schrems[65] que estudiaba derecho en un campus norteamericano, en una de sus clases, un abogado de Facebook respondió de forma muy evasiva a sus preguntas concretas sobre cómo la multinacional respetaba el derecho a la privacidad según la legislación europea. Y se lo tomó como algo personal.

Primero escribió una tesina sobre el tema. Después, a través de los mecanismos de "derecho al acceso a información" logró que la empresa le remitiera la información que tenían almacenada sobre él. Descubrió que eran más de 1.000 folios sobre una persona prácticamente anónima. Luego creó una plataforma de lucha. Y al final decidió llevar el caso a la justicia.

61. https://edwardsnowden.com/es/2013/11/05/special-source-operations-overview/

62. Foreign Intelligence Surveillance Act of 1978 (FISA) (Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. cap. 36

63. http://www.fisc.uscourts.gov/

64. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

65. http://internacional.elpais.com/internacional/2015/10/06/actualidad/1444145046_802400.html

El caso es sencillo: Schrems es usuario de Facebook desde 2008. Sus datos, como los de los europeos, se transmiten desde la filial de Facebook en Irlanda a los servidores que la empresa tiene en EEUU. Schrems presentó una denuncia ante la autoridad irlandesa de control, "considerando que, a la luz de las revelaciones realizadas en 2013 por Edward Snowden en relación con las actividades de los servicios de información de Estados Unidos, la normativa y la práctica de Estados Unidos no garantizaban una protección suficiente de los datos transferidos a ese país frente a las actividades de vigilancia por las autoridades públicas"[66].

En una primera instancia, las autoridades irlandesas desestimaron su denuncia porque la Comisión Europea había dejado claro que "en el marco del régimen denominado de «puerto seguro», Estados Unidos garantiza un nivel adecuado de protección de los datos personales transferidos"[67].

El Tribunal Supremo irlandés quería saber si el hecho de que exista esa directiva a nivel comunitario impide que las autoridades nacionales puedan investigar denuncias como concretas como la del ciudadano austriaco y, si fuera necesario, impedir que sus datos sean transferidos a un país que considera no seguro.

Schrems es un activista de 27 años que lucha contra la violación de la privacidad de Facebook y ha ganado una batalla histórica. "El Tribunal de Justicia declara inválida la Decisión de la Comisión que declaró que Estados Unidos garantiza un nivel de protección adecuado de los datos personales transferidos"[68] dice el dictamen emitido. Lo que quiere decir que la justicia europea ha tumbado la normativa vigente desde 2000 que permite la transferencia de información perteneciente a ciudadanos europeos a EEUU, al considerar que no se trata de un país seguro.

66. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

67. http://www.elmundo.es/tecnologia/2015/10/06/5613822ce2704ec1198b456e.html

68. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

2.3.- Sentencia del TJUE de 6 de octubre de 2015.

Llegamos al punto de inflexión que ha conmocionado la transferencia internacional de datos en lo que se refiere a la protección de los mismos. Como próximos letrados ejercientes, debemos estar al tanto de la historia que tiene detrás un caso como el que ha llevado a la sentencia del pasado mes de octubre, ya que quién sabe si algún día podamos tener algún caso remotamente parecido y más cuando viene de una serie de acontecimientos que han marcado un antes y un después en lo que se refiere a la protección de datos de carácter personal, haciendo que un país como Estados Unidos, fuente de progreso y modernización, sea considerado como un país excluido de la lista de países seguros para la transferencia ya que no cumple con los estándares de seguridad adecuados.

La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea[69], de los artículos 25, apartado 6, y 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[70], relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, p. 31), en su versión modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003 (DO L 284, p. 1) así como, en sustancia, la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46[71], 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 (DO L 215, p. 7)[72].

69. http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003 Publicado en «DOUE» núm. 83, de 30 de marzo de 2010, páginas 389 a 403

70. https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678 Publicado en «DOUE» núm. 281, de 23 de noviembre de 1995, páginas 31 a 50

71.http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

72.http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

Esa petición se ha presentado en el marco de un litigio entre el Sr. Schrems y el Data Protection Commissioner[73], acerca de la negativa de éste a instruir una reclamación presentada por el Sr. Schrems, basada en que Facebook Ireland Ltd[74] transfiere a Estados Unidos los datos personales de sus usuarios y los conserva en sus servidores situados en ese país.

Litigio principal y cuestiones prejudiciales[75]

"26 El Sr. Schrems, nacional austriaco residente en Austria, es usuario de la red Facebook (en lo sucesivo, «Facebook») desde 2008.

27 Toda persona residente en el territorio de la Unión que desee utilizar Facebook está obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento.

28 El 25 de junio de 2013 el Sr. Schrems presentó ante el comisario una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency (en lo sucesivo, «NSA»).

29 Considerando que no estaba obligado a investigar sobre los hechos denunciados por el Sr. Schrems en su reclamación, el comisario la desestimó por infundada. Apreció en efecto que no había pruebas de que la NSA hubiera accedido a los datos personales del interesado. El comisario añadió que las imputaciones formuladas por el Sr. Schrems en su reclamación no podían ser eficazmente aducidas, ya que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión 2000/520, en la que la Comisión había constatado que Estados Unidos garantizaba un nivel adecuado de protección.

75. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

30 El Sr. Schrems interpuso un recurso ante la High Court contra la decisión discutida en el litigio principal. Una vez examinadas las pruebas presentadas por las partes litigantes, ese tribunal apreció que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la Unión a Estados Unidos servían a finalidades necesarias e indispensables para el interés público. No obstante, el referido tribunal añadió que las revelaciones del Sr. Snowden habían demostrado que la NSA y otros organismos federales habían cometido «importantes excesos».

31 Ahora bien, según ese mismo tribunal, los ciudadanos de la Unión no disponen de ningún derecho efectivo a ser oídos. La supervisión de las acciones de los servicios de información se realiza a través de un procedimiento secreto y no contradictorio. Una vez transferidos los datos personales a Estados Unidos, la NSA y otros organismos federales, como el Federal Bureau of Investigation (FBI), pueden acceder a ellos en el contexto de la vigilancia y de las interceptaciones indiferenciadas que ejecutan a gran escala.

32 La High Court constató que el Derecho irlandés prohíbe la transferencia de datos personales fuera del territorio nacional, excepto cuando el tercer país interesado asegura un nivel de protección adecuado de la vida privada y de los derechos y libertades fundamentales. La importancia de los derechos al respeto de la vida privada y a la inviolabilidad del domicilio, protegidos por la Constitución irlandesa, exige que toda injerencia en esos derechos sea proporcionada y ajustada a las exigencias previstas por la ley.

33 Ahora bien, el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa. Para que las interceptaciones de comunicaciones electrónicas puedan ser consideradas conformes con esa Constitución, debe aportarse la prueba de que esas interceptaciones tienen carácter selectivo, de que la vigilancia de determinadas personas o de determinados grupos de personas está objetivamente justificada en interés de la seguridad nacional o de la represión de la delincuencia y de que existen garantías adecuadas y comprobables. Así pues, según la High Court, si el asunto principal se tuviera que resolver con fundamento exclusivo en el Derecho irlandés, se debería apreciar que, dada la existencia de serias dudas de que Estados Unidos garantice un nivel adecuado de protección de los datos personales, el comisario habría debido llevar a cabo una investigación sobre los hechos denunciados por el Sr. Schrems en su reclamación, y que la desestimó indebidamente.

34 No obstante, la High Court estima que este asunto atañe a la aplicación del Derecho de la Unión, en el sentido del artículo 51 de la Carta, por lo que la legalidad de

la decisión discutida en el asunto principal debe apreciarse a la luz del Derecho de la Unión. Ahora bien, según ese tribunal, la Decisión 2000/520 no se ajusta a las exigencias derivadas tanto de los artículos 7 y 8 de la Carta como de los principios enunciados por el Tribunal de Justicia en la sentencia Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238). El derecho al respeto de la vida privada garantizado por el artículo 7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros quedaría privado de alcance alguno si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas se rodeen de garantías adecuadas y comprobables.

35 La High Court observa además que, en realidad, el Sr. Schrems impugna en su recurso la licitud del régimen de «puerto seguro» establecido por la Decisión 2000/520, de la cual deriva la decisión discutida en el litigio principal. Así pues, aunque el Sr. Schrems no haya impugnado formalmente la validez de la Directiva 95/46 ni de la Decisión 2000/520, según ese tribunal se suscita la cuestión de si, en virtud del artículo 25, apartado 6, de la Directiva 95/46, el comisario estaba vinculado por la constatación realizada por la Comisión en esa Decisión, según la cual Estados Unidos garantiza un nivel de protección adecuado, o bien si el artículo 8 de la Carta autorizaba al comisario a separarse, en su caso, de esa constatación.

36 En esas circunstancias, la High Court decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

«1) En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legislación y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE

2) En caso contrario, ¿puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520”

A lo largo de la sentencia se argumenta del siguiente modo[76]:

"66 Por las anteriores consideraciones se ha de responder a las cuestiones planteadas que el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

Sobre la validez de la Decisión 2000/520

67 Según resulta de las explicaciones del tribunal remitente sobre las cuestiones planteadas, en el asunto principal el Sr. Schrems alega que el Derecho y las prácticas de Estados Unidos no garantizan un nivel de protección adecuado, en el sentido del artículo 25 de la Directiva 95/46. Como ha señalado el Abogado General en los puntos 123 y 124 de sus conclusiones, el Sr. Schrems manifiesta dudas, que ese tribunal parece compartir en sustancia, sobre la validez de la Decisión 2000/520. Siendo así, por las consideraciones expuestas en los apartados 60 a 63 de la presente sentencia, y para dar una respuesta completa al referido tribunal, es preciso apreciar si esa Decisión se ajusta a las exigencias derivadas de dicha Directiva entendida a la luz de la Carta.

Sobre las exigencias derivadas del artículo 25, apartado 6, de la Directiva 95/46

68 Como ya se ha observado en los apartados 48 y 49 de la presente sentencia, el artículo 25, apartado 1, de la Directiva 95/46 prohíbe las transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado.

76. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

69 No obstante, a efectos del control de esas transferencias el artículo 25, apartado 6, párrafo primero, de esa Directiva dispone que la Comisión «podrá hacer constar [...] que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 [de ese artículo], a la vista de su legislación interna o de sus compromisos internacionales […], a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

70 Es cierto que ni el artículo 25, apartado 2, de la Directiva 95/46 ni ninguna otra de sus disposiciones contienen una definición del concepto de «nivel de protección adecuado». En particular, el artículo 25, apartado 2, de esa Directiva se limita a enunciar que el carácter adecuado del nivel de protección que ofrece un tercer país «se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos», y enumera sin carácter exhaustivo las circunstancias que se deben considerar en esa apreciación.

71 No obstante, según resulta de los mismos términos del artículo 25, apartado 6, de la Directiva 95/46, esta disposición exige que un tercer país «garantice» un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales. Por otro lado, también conforme a esa disposición, el carácter adecuado del nivel de protección que ofrece un tercer país se ha de apreciar «a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

72 De esa forma, el artículo 25, apartado 6, de la Directiva 95/46 da cumplimiento a la obligación expresa de protección de los datos personales, prevista en el artículo 8, apartado 1, de la Carta, y pretende asegurar la continuidad del elevado nivel de protección en caso de transferencia de datos personales a un tercer país, como ha señalado el Abogado General en el punto 139 de sus conclusiones.

73 Es verdad que el término «adecuado» que figura en el artículo 25, apartado 6, de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo, como ha manifestado el Abogado General en el punto 141 de sus conclusiones, debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta. En efecto, a falta de esa exigencia el objetivo mencionado en el anterior apartado de la presente sentencia se frustraría. Además, el elevado nivel de protección garantizado por la Directiva 95/46 entendida a la luz de la Carta se podría

eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos.

74 De la redacción misma del artículo 25, apartado 6, de la Directiva 95/46 resulta que es el ordenamiento jurídico del tercer país al que se refiere la decisión de la Comisión el que debe garantizar un nivel de protección adecuado. Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión.

75 Siendo así, al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país, conforme al artículo 25, apartado 2, de la Directiva 95/46.

76 De igual modo, dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión en virtud del artículo 25, apartado 6, de la Directiva 95/46, comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido.

77 Además, como ha expuesto el Abogado General en los puntos 134 y 135 de sus conclusiones, al apreciar la validez de una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de la Directiva 95/46 también se han de tener en cuenta las circunstancias sobrevenidas después de su adopción.

78 En ese sentido es preciso observar que, dado el importante papel que cumple la protección de los datos personales en relación con el derecho fundamental al respeto de la vida privada, así como el gran número de personas cuyos derechos fundamentales pueden ser vulnerados en caso de transferencia de datos personales a un tercer país que no garantice un nivel de protección adecuado, la facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda reducida, por lo que se debe ejercer un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (véase por analogía la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48).

Sobre el artículo 1 de la Decisión 2000/520

79 La Comisión manifestó en el artículo 1, apartado 1, de la Decisión 2000/520 que los principios que figuran en el anexo I de ésta, aplicados de conformidad con la orientación que proporcionan las FAQ enunciadas en el anexo II de la misma Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos. De esa disposición resulta que tanto esos principios como las FAQ han sido publicados por el Departamento de Comercio estadounidense.

80 La adhesión de una entidad a los principios de puerto seguro se lleva a cabo conforme a un sistema de autocertificación, como resulta del artículo 1, apartados 2 y 3, de esa Decisión, en relación con la FAQ nº 6 que figura en el anexo II de ésta.

81 Aunque el recurso por un tercer país a un sistema de autocertificación no es por sí mismo contrario a la exigencia enunciada en el artículo 25, apartado 6, de la Directiva 95/46 de que el tercer país considerado garantice un nivel de protección adecuado «a la vista de su legislación interna o de sus compromisos internacionales», la fiabilidad de ese sistema en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales.

82 En el presente asunto, en virtud del anexo I, párrafo segundo, de la Decisión 2000/50, los principios de puerto seguro «son de utilización exclusiva de las entidades estadounidenses que reciben datos personales de la Unión Europea, al efecto de reunir los requisitos de "puerto seguro" y obtener la correspondiente presunción de "adecuación"». Por tanto, esos principios son aplicables únicamente a las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión, sin que se exija que las autoridades públicas estadounidenses se sometan a esos principios.

83 Además, en virtud del artículo 2 de la Decisión 2000/520, ésta «se refiere únicamente a la adecuación de la protección proporcionada en Estados Unidos de América con arreglo a los principios [de puerto seguro] y su aplicación de conformidad con las FAQ a fin de ajustarse a los requisitos del apartado 1 del artículo 25 de la Directiva [95/46]», sin contener no obstante las constataciones suficientes sobre las medidas con las que Estados Unidos garantiza un nivel de protección adecuado, en el sentido del artículo 25, apartado 6, de esa Directiva, a la vista de su legislación interna o de sus compromisos internacionales.

84 A ello se añade que, conforme al anexo I, párrafo cuarto, de la Decisión 2000/520, la aplicabilidad de esos principios puede limitarse, en especial, por «las exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]», así como por «disposición legal o reglamentaria, o jurisprudencia, que originen conflictos de obligaciones o autorizaciones [explícitas], siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones».

85 En ese sentido, en el título B de su anexo IV la Decisión 2000/520 pone de relieve, respecto a los límites a los que está sometida la aplicabilidad de los principios de puerto seguro, que «es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro».

86 Así pues, la Decisión 2000/520 reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]» sobre los principios de puerto seguro, primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten por tanto incompatibles con ellas.

87 Dado el carácter general de la excepción prevista en el anexo I, párrafo cuarto, de la Decisión 2000/520, ésta hace posibles así injerencias, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos, en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos. En ese sentido, para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 33 y la jurisprudencia citada).

88 Además, la Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional.

89 Se añade a ello el hecho de que la Decisión 2000/520 no pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza. Como ha expuesto el Abogado General en los puntos 204 a 206 de sus conclusiones, los mecanismos de arbitraje privado y los procedimientos ante la Comisión Federal de Comercio, cuyas facultades, descritas en particular en las FAQ nº 11 que figuran en el anexo II de esa Decisión, se limitan a los litigios comerciales, atañen al cumplimiento por las empresas estadounidenses de los principios de puerto seguro, y no se pueden aplicar en litigios concernientes a la legalidad de injerencias en los derechos fundamentales derivadas de medidas de origen estatal.

90 Por otro lado, el análisis precedente de la Decisión 2000/520 se confirma por la apreciación que la misma Comisión ha realizado sobre la situación resultante de la aplicación de esa Decisión. En efecto, en particular en los puntos 2 y 3.2 de la Comunicación COM(2013) 846 final y en los puntos 7.1, 7.2 y 8 de la Comunicación COM(2013) 847 final, cuyo contenido se expone respectivamente en los apartados 13 a 16, y 22, 23 y 25 de la presente sentencia, la Comisión constató que las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional. De igual modo, la Comisión apreció que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión.

91 En lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión, según reiterada jurisprudencia del Tribunal de Justicia, una normativa de ésta que haga posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a ellos (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55 y la jurisprudencia citada).

92 Además, y sobre todo, la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones a la protección de los datos

personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 52 y la jurisprudencia citada).

93 Pues bien, no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización [véase en ese sentido, acerca de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, p. 54), la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 57 a 61].

94 En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta (véase, en ese sentido, la sentencia Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 39).

95 De igual manera, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta. En efecto, el artículo 47, párrafo primero, de ésta establece que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva, respetando las condiciones establecidas en dicho artículo. En ese sentido, la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho (véanse, en ese sentido, las sentencias Les Verts/Parlamento, 294/83, EU:C:1986:166, apartado 23; Johnston, 222/84, EU:C:1986:206, apartados 18 y 19; Heylens y otros, 222/86, EU:C:1987:442, apartado 14, y UGT-Rioja y otros, C-428/06 a C-434/06, EU:C:2008:488, apartado 80).

96 Como se ha apreciado en particular en los apartados 71, 73 y 74 de la presente sentencia, la adopción por la Comisión de una decisión en virtud del artículo 25,

apartado 6, de la Directiva 95/46 requiere la constatación debidamente motivada por esa institución de que el tercer país considerado garantiza efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión, según resulta de los anteriores apartados de esta sentencia.

97 Ahora bien, se ha de observar que la Comisión no manifestó en la Decisión 2000/520 que Estados Unidos «garantiza» efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales.

98 En consecuencia, y sin que sea preciso apreciar el contenido de los principios de puerto seguro, se debe concluir que el artículo 1 de esa Decisión vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa.

Sobre el artículo 3 de la Decisión 2000/520

99 De las consideraciones expuestas en los apartados 53, 57 y 63 de la presente sentencia se sigue que, en virtud del artículo 28 de la Directiva 95/46, entendido a la luz del artículo 8 de la Carta, las autoridades nacionales de control deben poder examinar con toda independencia cualquier solicitud de protección de los derechos y libertades de una persona frente a un tratamiento de datos personales que la afecte. Así es, en particular, cuando esa persona suscite con ocasión de su solicitud interrogantes sobre la compatibilidad de una decisión de la Comisión adoptada en virtud del artículo 25, apartado 6, de esa Directiva con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

100 No obstante, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 establece una regulación específica de las facultades de las que disponen las autoridades nacionales de control ante una constatación realizada por la Comisión sobre el nivel de protección adecuado, en el sentido del artículo 25 de la Directiva 95/46.

101 De esa forma, a tenor de dicha disposición las referidas autoridades, «sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva [95/46], […] podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios [de la Decisión 2000/520]», de manera restrictiva, ya que sólo es posible la intervención a partir de un alto umbral de condiciones. Aunque esa disposición no enerva las facultades de esas autoridades para tomar medidas encaminadas a asegurar el cumplimiento de las

disposiciones nacionales adoptadas en aplicación de esa Directiva, excluye en cambio la posibilidad de que esas autoridades tomen medidas con objeto de asegurar el cumplimiento del artículo 25 de la misma Directiva.

102 Por tanto, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 debe entenderse en el sentido de que priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46, en el supuesto de que una persona alegue, con ocasión de una solicitud basada en esa disposición, factores que puedan afectar a la compatibilidad de una decisión de la Comisión, que haya constatado con fundamento en el artículo 25, apartado 6, de esa Directiva que un tercer país garantiza un nivel de protección adecuado, con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

103 Ahora bien, la facultad de ejecución atribuida a la Comisión por el legislador de la Unión en el artículo 25, apartado 6, de la Directiva 95/46 no confiere a esa institución la competencia para restringir las facultades de las autoridades nacionales de control a las que se refiere el anterior apartado de esta sentencia.

104 Siendo así, es preciso apreciar que, al adoptar el artículo 3 de la Decisión 2000/520, la Comisión excedió los límites de la competencia que le atribuye el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y que dicho artículo 3 es inválido por esa causa.

105 Toda vez que los artículos 1 y 3 de la Decisión 2000/520 son indisociables de los artículos 2 y 4 y de los anexos de ésta, su invalidez tiene el efecto de afectar a la validez de esa Decisión en su conjunto.

106 Por todas las consideraciones precedentes se debe concluir que la Decisión 2000/520 es inválida.

Llegando al fallo, en virtud de todo lo expuesto, el Tribunal de Justicia (Gran Sala) declara:

1) El artículo 25, apartado 6, de la de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su versión modificada por el Reglamento (CE) nº 882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003, entendido a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que una Decisión adoptada en virtud de la referida

disposición, como la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, 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, por la que la Comisión Europea constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, en su versión modificada, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado.

2) La Decisión 2000/520 es inválida."

Con este fallo se deja sin efecto el marco en el que se creían protegidos los datos de carácter personal que se transferían con Estados Unidos por lo que desde la Comisión se tuvieron que revisar "el Derecho y las prácticas vigentes en los Estados Unidos, incluidos estos compromisos y declaraciones oficiales." Concluyendo finalmente la Comisión que "los Estados Unidos garantizan un nivel adecuado de protección de los datos personales transferidos en el marco del Escudo de la privacidad UE-EE. UU. desde la Unión a entidades autocertificadas establecidas en los Estados Unidos." No es sino a través de una nueva Decisión que fue adoptada el pasado mes de julio. [77]

77. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES

3.- 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-EEUU.[78]

"A raíz de la sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems, estas conversaciones se intensificaron con miras a adoptar una nueva decisión de adecuación que cumpliera lo dispuesto en el artículo 25 de la Directiva 95/46/CE, tal como ha sido interpretado por el Tribunal de Justicia. Los principios de privacidad, así como los compromisos y declaraciones oficiales de diversas autoridades estadounidenses recogidos en los documentos de los anexos I y III a VII, constituyen el denominado «Escudo de la privacidad UE-EEUU.»."[79]

Pues bien, que se entiendo por escudo de privacidad, según la Decisión 1250/2016 "El Escudo de la privacidad UE-EEUU se basa en un sistema de autocertificación por el que las entidades estadounidenses se comprometen a cumplir una serie de principios de protección de la vida privada, a saber, los principios marco del Escudo de la privacidad UE-EEUU, incluidos los principios complementarios establecidos por el Departamento de Comercio de Estados Unidos y enumerados en el anexo II de la presente Decisión. Se aplica tanto a los responsables como a los encargados del tratamiento (agentes), con la particularidad de que los encargados deben estar obligados contractualmente a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la UE y asistir a este último a responder a las personas físicas que ejerzan sus derechos con arreglo a los principios"[80]

78. http://www.boe.es/doue/2016/207/L00001-00112.pdf

79. http://www.boe.es/doue/2016/207/L00001-00112.pdf

80. http://www.boe.es/doue/2016/207/L00001-00112.pdf

El funcionamiento de este escudo es el que queda recogido en la guía que ha elaborado sobre él la Comisión Europea, "Para transferir datos personales de la UE a los EEUU se dispone de distintas herramientas como las cláusulas contractuales, las normas corporativas vinculantes y el escudo de la privacidad. Para utilizar el escudo de la privacidad, las empresas estadounidenses deben primero afiliarse a ese sistema en el Departamento de Comercio de los EEUU. Las obligaciones que contraen las empresas afiliadas al escudo de la privacidad se recogen en los «principios de privacidad». El citado Departamento es responsable de gestionar y administrar el escudo de la privacidad y de velar por que las empresas cumplan sus compromisos. Para poder obtener una certificación, las empresas deberán tener una política de privacidad acorde con los principios de privacidad y renovar su «afiliación» al escudo de la privacidad con carácter anual. De no hacerlo, dejarán de poder recibir y usar los datos personales de la UE con arreglo a ese marco."[81]

Como letrados, podemos tener clientes que necesiten saber si los datos de carácter personal que van a transferir están bajo este Escudo, "para averiguar si una empresa de la UE está afiliada al escudo de la privacidad, puede consultar la lista correspondiente en el sitio web del Departamento de Comercio[82]. En ella figuran los datos de todas las empresas que participan en el escudo de la privacidad, el tipo de datos personales que utilizan y la clase de servicios que ofrecen. También se puede consultar una lista de las empresas que han dejado de pertenecer al escudo de la privacidad y que, por lo tanto, no tienen ya derecho a recibir sus datos personales con arreglo a ese mecanismo. Además, estas empresas solo podrán conservar sus datos personales si se comprometen, ante el Departamento de Comercio, a seguir aplicando los principios de privacidad."[83]

81. http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

82. https://www.privacyshield.gov/welcome

83. http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

Además debemos saber que existen una serie de obligaciones que deben cumplir estas empresas[84]:

1. Derecho a ser informado
2. Limitaciones del uso de sus datos con fines distintos
3. Minimización de los datos y obligación de conservar sus datos únicamente durante el tiempo necesario
4. Obligación de asegurar sus datos
5. Obligación de proteger sus datos si se transfieren a otra empresa
6. Derecho de acceso a los datos y de rectificación de los mismos
7. Derecho a presentar una reclamación y a obtener reparación
8. Reparación en caso de acceso por parte de las autoridades públicas de los EE. UU

Desde un punto de vista práctico, si un cliente nos presenta el asunto de que ha visto violado una de esas obligaciones, debemos ser capaces de darle una respuesta coherente, ésta no sería otra que acudir a los mecanismos que se prevén en la Decisión de julio de 2016[85].

"El primero de ellos es si la empresa está afiliada al escudo de privacidad de los EEUU. Toda empresa debe siempre facilitar los datos de un responsable con el que podamos ponernos en contacto directamente para cualquier consulta o reclamación. La empresa debe responder en un plazo de 45 días a partir de la recepción de la reclamación. En esa respuesta debe indicar si la reclamación está fundada y, en tal caso, la reparación que ofrece. La empresa está obligada a investigar todas las reclamaciones que reciba, salvo aquellas que a todas luces carezcan de fundamento.

En caso de que la empresa haya escogido un organismo independiente de resolución alternativa de litigios, en el sitio web de la empresa deberá facilitar la información y un enlace al sitio web del organismo independiente de resolución alternativa de litigios, en el que habrán de figurar todos los datos sobre los servicios que este ofrece, incluidos los procedimientos aplicables. Estos organismos deben tener la potestad de aplicar medios de reparación y sanciones efectivos que aseguren que la empresa afiliada al escudo de la privacidad cumple su obligación de proteger los datos personales."[86]

84. http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

85. http://www.boe.es/doue/2016/207/L00001-00112.pdf

86. http://www.boe.es/doue/2016/207/L00001-00112.pdf

"En principio, las empresas afiliadas al escudo de la privacidad tienen la posibilidad de optar por una autoridad de protección de datos de la UE como su mecanismo de recurso independiente. Sin embargo, cuando una empresa maneja datos de recursos humanos, la supervisión de la APD es obligatoria. Esto significa que, como empleado, siempre se puede acudir a la ADP local en caso de reclamación relativa a la transferencia de datos profesionales a una empresa afiliada al escudo de la privacidad. Además, incluso si una APD carece de competencias de supervisión sobre una empresa concreta afiliada al escudo de la privacidad, siempre nos podemos dirigir a la APD, la cual puede remitir su reclamación a una de las autoridades competentes de los EEUU.

Las APD entregarán su dictamen a la empresa lo antes posible y, en cualquier caso, dentro de un plazo de 60 días desde la recepción de la reclamación. Se nos informará sobre dicho dictamen, que se hará público en la medida de lo posible. A continuación, la empresa dispone de 25 días para cumplir lo dictaminado; de no hacerlo así, la APD podría remitir el asunto a la Comisión Federal de Comercio de los EEUU para la posible adopción de medidas coercitivas. También puede comunicar al Departamento de Comercio la negativa de la empresa a ajustarse al dictamen de la APD, lo que podría desembocar, de persistir la empresa en el incumplimiento, en su eliminación de la lista del escudo de la privacidad.

Además, si la reclamación pone de manifiesto que la transferencia de los datos personales a la empresa afiliada al escudo de privacidad infringe las normas de protección de datos de la UE, la APD puede también actuar contra la empresa de la UE que envíe los datos y, en caso necesario, ordenar la suspensión de dicha transferencia. Se incluyen entre estos casos aquellos en los que la empresa de la UE tenga motivos para sospechar que la empresa afiliada al escudo de la privacidad está incumpliendo los principios de privacidad.

Incluso si una APD carece de competencias de supervisión sobre la empresa afiliada al escudo de privacidad respecto de la que usted formula su reclamación, puede remitirla al Departamento de Comercio de los EEUU, recurrirá para ello al punto de contacto específico responsable del contacto directo con las APD. El Departamento de Comercio examinará la reclamación y ofrecerá una respuesta a la APD en un plazo de 90 días. El Departamento de Comercio también puede transmitir las reclamaciones a la Comisión Federal de Comercio."[87]

87. http://www.boe.es/doue/2016/207/L00001-00112.pdf

"Otra posibilidad es la Comisión Federal de Comercio. Podemos presentar la reclamación directamente a la Comisión Federal de Comercio de los EEUU por los mismos cauces que los ciudadanos estadounidenses[88]. La Comisión Federal de Comercio examinará también las reclamaciones que reciba del Departamento de Comercio de los EEUU, las APD de la UE y los organismos independientes de resolución alternativa de litigios. Al igual que el Departamento de Comercio, la Comisión Federal de Comercio ha creado un punto de contacto específico para establecer contacto directo con las APD de la UE a fin de facilitar las consultas y reforzar la cooperación en la tramitación de las reclamaciones particulares.

Por último, el Panel (comisión de arbitraje) del escudo de la privacidad. Si la reclamación sigue total o parcialmente sin resolver tras el uso de los demás mecanismos de reparación, o si no hemos quedado satisfechos con el curso dado a nuestra reclamación, tenemos derecho a obtener reparación mediante otra opción: el arbitraje vinculante.

Algunas consideraciones prácticas importantes a la hora de acudir al arbitraje, solo se puede acudir como particular. Toda empresa afiliada al escudo de la privacidad está obligada a arbitrar las reclamaciones cuando se invoque ese derecho. Sin embargo, solo se podrá hacer una vez se hayan agotado otras vías de recurso, como las ofrecidas por la empresa, el organismo independiente de resolución alternativa de litigios o el Departamento de Comercio. Hay otras situaciones en que no se puede recurrir al Panel del escudo de la privacidad, concretamente, si la reclamación ha sido ya sometida anteriormente a un procedimiento de arbitraje; si un órgano jurisdiccional se ha pronunciado ya, en un procedimiento del que hayamos sido parte; si las partes ya han llegado a un acuerdo en cuanto a la reclamación; o si la APD puede resolver la reclamación directamente ante la empresa. No obstante, las investigaciones de la Comisión Federal de Comercio pueden desarrollarse de forma paralela al arbitraje.

La forma de iniciar el procedimiento es en primer lugar notificar formalmente su intención a la empresa. La notificación deberá incluir un resumen de las medidas ya adoptadas para resolver su reclamación y una descripción de la presunta infracción. También se pueden presentar justificantes o textos jurídicos relacionados con su reclamación."[89]

88. www.ftc.gov/complaint

89. http://www.boe.es/doue/2016/207/L00001-00112.pdf

El arbitraje tendrá lugar en los Estados Unidos, dado que la empresa respecto de la que presenta la reclamación tiene allí su sede. Dicho esto, existen varios aspectos favorables al consumidor, nuestro cliente, que nos serán de gran utilidad:

1. El derecho a solicitar la asistencia de la autoridad de protección de datos para preparar la reclamación;
2. La posibilidad de comparecer en el procedimiento por teléfono o videoconferencia, de forma que no hay obligación de estar físicamente presente en los EEUU;
3. La posibilidad de obtener, de forma gratuita, servicios de interpretación y de traducción de los documentos del inglés a otra lengua;
4. Los costes del arbitraje (excepto nuestros honorarios) se compensarán a partir de un fondo específicamente creado por el Departamento de Comercio y se financiarán con cargo a las contribuciones anuales de las empresas afiliadas al escudo de la privacidad.

El procedimiento de arbitraje habrá concluido en un plazo de 90 días a partir de la fecha en que hayamos enviado la notificación a la empresa.[90]

Si el Panel del escudo de la privacidad constata una infracción de los principios de privacidad, se pueden adoptar medidas de reparación, como el acceso a los datos personales o la rectificación, supresión o devolución de los mismos. Aunque el Panel no puede conceder una indemnización pecuniaria, tenemos la posibilidad de reclamarla ante los tribunales. De no estar satisfechos con el resultado del arbitraje, podemos impugnarlo con arreglo a la legislación estadounidense, a saber, la Ley de Arbitraje.[91]

Por último, se puede recurrir al Defensor del Pueblo estadounidense[92], es un alto funcionario del Departamento de Estado de los Estados Unidos. “En el desempeño de sus tareas, dando curso a las reclamaciones recibidas, el Defensor del Pueblo colaborará estrechamente con otros organismos independientes de supervisión e investigación y obtendrá de ellos toda la información necesaria para dar su respuesta en cuanto a la compatibilidad de la vigilancia con la legislación estadounidense. Esos organismos son los encargados de supervisar a los diversos servicios de inteligencia de los EE. UU.”[93]

90. http://www.boe.es/doue/2016/207/L00001-00112.pdf

91. https://www.law.cornell.edu/uscode/text/9

92. https://es.sba.gov/ombudsman

93. http://www.boe.es/doue/2016/207/L00001-00112.pdf

El procedimiento se inicia por solicitud y posterior investigación tras la posible subsanación de errores en la solicitud, dando una respuesta de si se han violado o no los derechos de nuestro posible representado, pero lo que nunca comunicará el Defensor del Pueblo es si nuestro cliente ha sido objeto de vigilancia por parte de los servicios secretos o de inteligencia de los Estados Unidos.

Una vez que sabemos qué se puede hacer, vemos ejemplos prácticos a modo de acercamiento, como dice Jesús P. López Pelaz Director de Abogado Amigo en su artículo de 9 de octubre de 2015[94], toda la situación creada con la sentencia de octubre de 2015 impacta negativamente en la economía europea "Este asunto afecta a la generalidad del tejido empresarial de la UE. Miles de empresas de todo tipo y tamaño utilizan recursos situados en EEUU (y/o se valen de proveedores europeos que usan tales recursos en Norteamérica) para almacenar y tratar datos personales en sistemas de recursos humanos, CRM, etc. Son servicios prestados por proveedores adheridos al esquema de Puerto Seguro. Hasta ahora, estas empresas de la UE estaban tranquilas porque los flujos de datos personales a estos proveedores en EEUU estaban legitimados por la Decisión de Puerto Seguro. Ahora, ya no lo están y tienen que tomar medidas que no son inocuas a nivel económico. Al margen de los costes, la declaración de invalidez de la Decisión de Puerto Seguro también impacta en los ingresos. Empresas de la EU pueden dejar de ser competitivas si no pueden acceder a tecnologías situadas en EEUU de forma alguna o a un precio razonable."

Tras el primer revuelo tanto entre los particulares como entre las empresas, la AEPD aclaró, como recoge Michael Mcloughlin en su artículo del 9 de diciembre de 2015[95], "lo único que se ha hecho es establecer una comunicación con las empresas que trataban datos personales a través de servicios que hacía uso de la Declaración de Puerto Seguro -como Google Drive y Dropbox- tras la sentencia del TSJE. Por tanto, no ha se les ha pedido que dejen de utilizar estos servicios, sino que requieran a su proveedor una solución adaptada." Es decir, no queda prohibido el uso de estas plataformas, que como profesionales o a modo particular hemos podido usar o usamos de hecho en la actualidad, sino que habrían de dar una solución al problema concreto, soluciones que quedan configuradas en la Decisión antes analizada en el cuerpo de este trabajo.

94. http://www.abogadoamigo.com/puerto-seguro/

95.http://www.elandroidelibre.com/2015/12/no-nadie-ha-prohibido-el-uso-de-google-apps-y-dropbox-en-espana.html

Por su parte, en palabras del abogado Javier Ponfeta, las medianas y pequeñas empresas poco pueden hacer a la hora de negociar los contratos que se han de firmar de acuerdo con el Privacy Shield, el Escudo, por lo que a la pregunta de qué pueden hacer si se pierden esos datos, responde que: "En general, y a la vista de las cláusulas y garantías de los contratos, en mi opinión en los casos en que se cumplen las medidas de seguridad, la compensación o indemnizaciones económicas son totalmente insuficientes para cubrir los daños, y por otro lado los contratos se someten a legislación y tribunales extranjeros. Los costes de demandar en EE.UU. son muy elevados, fuera del alcance de la mayoría de la pequeñas y medianas empresas."[96]

4.- Conclusiones

A lo largo de este trabajo he intentado dar una visión práctica a la hora de abordar un caso que contenga alguna circunstancia en lo que se refiere a la protección de datos y de cómo las sentencias y distintas decisiones de los diferentes órdenes jurisprudenciales pueden modificar el terreno de juego de un mes a otro.

Empezábamos con la seguridad de que la transmisión de datos de carácter personal se realizaba bajo unos parámetros adecuados a lo que entendemos por seguros, con las distintas revelaciones vertidas por Snowden y con el "caso Facebook" se comprobó como esa supuesta seguridad no era tal y se llegó a la Sentencia de 6 de octubre de 2015, en la que como conclusión debemos sacar que todo es como parece, en Europa tenemos, o debería decir teníamos unas ideas de respeto por la privacidad, de lo que se considera privado y público que en conflicto directo con la mentalidad de otros países como puede ser Estados Unidos, quedan diluidas en lo que se refiere a lo que ellos llaman "seguridad nacional", es decir, un casi total y absoluto acceso a la vida privada de las personas no solo residentes sino turistas, y más aún y en lo que se refiere este trabajo, europeos que confían en que sus datos estarán seguros y recibirán un trato adecuado, cuando como veíamos en las distintas publicaciones de The Guardian o el Washington Post, las distintas agencias norteamericanas han ido recopilando datos de los ciudadanos europeos a lo largo de los años.

96. http://www.genbeta.com/a-fondo/nube-y-proteccion-de-datos-que-deberia-saber-una-empresa-al-usar-dropbox-o-google-drive

Llegados a este punto, y viendo el malestar y posible cascada de demandas que por parte de la población podrían sufrir las empresas privadas que tienen su sede en Estados Unidos, el pasado mes de julio se llegó tras las negociaciones oportunas, a la Decisión de Ejecución 2016/1250, en la cual se confiere a EEUU el nivel adecuado de seguridad que se le había retirado, pero no al país como tal, sino individualizando a las empresas que quieran obtener esta garantía para sus clientes, debiendo comprometerse a la realización de las buenas prácticas que se suponen se cumplen en Europa, firmando una serie de documentos accesibles a todas ellas en las páginas oficiales y dándoles facilidades a las mismas para su realización.

Pues bien, como letrados, o futuros letrados, se nos dan unas pautas de cómo abordar el caso en que un cliente vea menoscabados sus derechos, en la Decisión de Ejecución, se nos dan las claves para la llevanza de una reclamación, reclamación que cuenta con plazos muy breves para lo que implican, ya que se brinda la posibilidad de acudir incluso a autoridades de control norteamericanas, sin cargo alguno más que el del letrado, llegando en último término a dar la posibilidad de acudir al arbitraje, siempre que se hayan intentado otros medios para la resolución del conflicto.

En mi opinión, estos métodos que promulga la Decisión, no son más que una argamasa de trámites para que el particular vea disipada su decisión de pelear contra una empresa, que ya no solo está en España o en Europa, sino al otro lado del Atlántico, en otro idioma, como letrados debemos estar preparados para este tipo de casos, son un campo casi sin explorar, se requiere tener conocimientos de idiomas, informática y otras disciplinas que seguro quedan fuera del alcance la gran mayoría de letrados, pero para eso estamos las nuevas generaciones de abogados, para ilustrarnos en lo que la globalización conlleva, poder tener un litigio en Estados Unidos y otro en un Juzgado de Primera Instancia de una ciudad como Salamanca. Y este trabajo no es otra cosa que un acercamiento a esta realidad en la que nos tendremos que mover y que la práctica nos puede dar la posibilidad de abordar.

Bibliografía

AGENCY, N. S. (s.f.). *nsa.gov*. Recuperado el 25 de 10 de 2016, de https://www.nsa.gov

AGPD. (s.f.). *AGPD.es.* Recuperado el 20 de 10 de 2016, de http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

agpd.es. (s.f.). Recuperado el 20 de 10 de 2016, de www.agpd.es

backbonejs.org. (s.f.). Recuperado el 26 de 10 de 2016, de http://backbonejs.org/

Biografiasyvidas. (s.f.). *biografiasyvidas.com*. Recuperado el 26 de 10 de 2016, de http://www.biografiasyvidas.com/biografia/b/bush_george.htm

BOE. (29 de Diciembre de 1978). *Agencia Estatal BOE.* Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229

BOE. (23 de noviembre de 1995). *boe.es.* Recuperado el 29 de 10 de 2016, de https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678 Publicado en «DOUE» núm. 281, de 23 de noviembre de 1995, páginas 31 a 50

BOE. (14 de Diciembre de 1999). *Agencia Estatal BOE.* Recuperado el 6 de Octubre de 2016, de https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

BOE. (31 de Julio de 2006). *Agencia Estatla BOE.* Obtenido de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2006-13849

BOE. (19 de Enero de 2008). *Agencia Estatal BOE.* Obtenido de http://boe.es/diario_boe/txt.php?id=BOE-A-2008-979

BOE. (30 de marzo de 2010). *boe.es.* Recuperado el 29 de 10 de 2016, de http://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70003 Publicado en «DOUE» núm. 83, de 30 de marzo de 2010, páginas 389 a 403

CIA. (s.f.). *cia.gov/es*. Recuperado el 25 de 10 de 2016, de https://www.cia.gov/es

CNN, B. S. (s.f.). *cnnespanol.cnn.com.* Recuperado el 21 de 10 de 2016, de http://cnnespanol.cnn.com/2013/06/10/quien-es-edward-snowden-el-hombre-que-filtro-datos-secretos-de-la-nsa/

ComisiónEuropea. (s.f.). *AGPD.es.* Recuperado el 21 de 10 de 2016, de https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/Dec_2004_915_CE_271204_vers_consoli.pdf

ComisiónEuropea. (s.f.). *boe.es.* Recuperado el 29 de 10 de 2016, de http://www.boe.es/doue/2016/207/L00001-00112.pdf

ComisiónEuropea. (s.f.). *ec.europa.eu.* Recuperado el 29 de 10 de 2016, de http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_es.pdf

ConsejoDeEuropa. (1995). *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al*

tratamiento de datos personales y a la libre circulación de estos datos. Recuperado el 16 de 10 de 2016

DepartamentodeComercioEEUU. (s.f.). *privacyshield.gov.* Recuperado el 12 de 11 de 2016, de https://www.privacyshield.gov/welcome

edwardsnowden.com. (s.f.). Recuperado el 27 de 10 de 2016, de https://edwardsnowden.com/es/2013/11/05/special-source-operations-overview/

El mundo, P. R. (s.f.). *elmundo.es.* Recuperado el 28 de 10 de 2016, de http://www.elmundo.es/tecnologia/2015/10/06/5613822ce2704ec1198b456e.html

El País, G. G. (s.f.). *elpais.com.* Recuperado el 28 de 10 de 2016, de http://internacional.elpais.com/internacional/2013/06/10/actualidad/1370865085_661307.html

fisc.uscourts.gov. (s.f.). Recuperado el 27 de 10 de 2016, de http://www.fisc.uscourts.gov/

FM, Y. (s.f.). *genbeta.com.* Recuperado el 18 de 11 de 2016, de http://www.genbeta.com/a-fondo/nube-y-proteccion-de-datos-que-deberia-saber-una-empresa-al-usar-dropbox-o-google-drive

ftc.gov. (s.f.). Recuperado el 12 de 11 de 2016, de www.ftc.gov/complaint

GobiernoEEUU. (s.f.). *fas.org.* Recuperado el 26 de 10 de 2016, de https://fas.org/irp/agency/doj/fisa/index.html

GobiernoEEUU. (s.f.). *justice.gov.* Recuperado el 26 de 10 de 2016, de https://www.justice.gov/archive/ll/

GobiernoEEUU. (s.f.). *law.cornell.edu.* Recuperado el 13 de 11 de 2016, de https://www.law.cornell.edu/uscode/text/9

LESMES SERRANO, C. B. (2008). *Ley de protección de datos. Ánalisis y comentario de su jurisprudencia .* LEX NOVA.

Mcloughlin, M. (s.f.). *elandroidelibre.com.* Recuperado el 16 de 11 de 2016, de http://www.elandroidelibre.com/2015/12/no-nadie-ha-prohibido-el-uso-de-google-apps-y-dropbox-en-espana.html

Parlamento Europeo, C. d. (s.f.). *eur-lex.es.* Recuperado el 20 de 10 de 2016, de http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478256785205&uri=CELEX:32000D0520

Pelaz, J. P. (s.f.). *abogadoamigo.com.* Recuperado el 15 de 11 de 2016, de http://www.abogadoamigo.com/puerto-seguro/

sba.gov/ombudsman. (s.f.). Recuperado el 12 de 11 de 2016, de https://es.sba.gov/ombudsman

TC. (s.f.). *BOE.es.* Recuperado el 18 de 10 de 2016, de https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

TC. (s.f.). *BOE.es.* Recuperado el 18 de 10 de 2016, de https://www.boe.es/diario_boe/txt.php?id=BOE-T-1991-15519

TC. (s.f.). *congreso.es.* Recuperado el 19 de 10 de 2016, de http://www.congreso.es/constitucion/ficheros/sentencias/stc_083_1984.pdf

TEDH. (s.f.). *curia.europa.eu.* Recuperado el 28 de 10 de 2016, de http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

TEDH. (s.f.). *http://www.echr.coe.int/Pages/home.aspx?p=home.* Recuperado el 17 de 10 de 2016, de http://www.mjusticia.gob.es/cs/Satellite/Portal/1292427055095?blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadername2=Grupo&blobheadervalue1=attachment%3B+filename%3DSentencia_DE_LA_FLOR_CABRERA_c._Espa%C3%B1a.pdf&blobheadervalue2

TEDH. (s.f.). *hudoc.echr.coe.* Recuperado el 17 de 10 de 2016, de http://hudoc.echr.coe.int/eng#{"fulltext":["funkeof france"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-57809"]}

TEDH. (s.f.). *hudoc.echr.coe.* Recuperado el 17 de 10 de 2016, de http://hudoc.echr.coe.int/eng#{"fulltext":["finlande25fevrier1997"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-62593"]}

TEDH. (s.f.). *sbdp.org.br.* Recuperado el 18 de 10 de 2016, de http://www.sbdp.org.br/arquivos/material/1706_ASE_OF_VON_HANNOVER_v._GERMANY_No._2__Spanish_Translation_by_the_COEECHR_and_Thomson_Reuters_Aranzad.pdf.

TheGuardian. (s.f.). *theguardian.com.* Recuperado el 26 de 10 de 2016, de https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

TJUE. (s.f.). *curia.europa.eu.* Recuperado el 15 de 10 de 2016, de http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=ES Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014. Digital Rights Ireland Ltd (C-293/12) contra Minister for Communications, Marine and Natural Resources y otros y Kärntner

WashingtonPost. (s.f.). *washingtongpost.com*. Recuperado el 26 de 10 de 2016, de https://www.washingtongpost.com/