VICISITUDES DE LOS INTENTOS DE LA COMISIÓN EUROPEA POR FACILITAR LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES HACIA ESTADOS UNIDOS.

ENSEÑANZAS QUE NOS DEJAN.

AUTORA:
Nombres: CAROLINA MARCELA
Apellidos: REYES KAHANSKY

INTRODUCCIÓN

La protección de datos personales es un derecho fundamental garantizado en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea[1] (que tiene el mismo valor que los Tratados Fundamentales según el art. 6.1 del Tratado de la Unión Europea); si bien, a diferencia del resto de derechos fundamentales de la Carta, este derecho constituye una competencia que los Estados miembros han atribuido a la Unión a través del art. 16 del Tratado de Funcionamiento de la Unión Europea, que ordena al Parlamento Europeo y al Consejo que dicten normas para brindarle protección en todos los ámbitos de aplicación del derecho de la Unión. Por ello éste garantiza a las personas físicas un alto nivel de protección en relación con los tratamientos de sus datos personales, que se asienta, entre otros factores, en una rigurosa responsabilidad de los agentes que intervienen en dichos tratamientos.

Desde el 24 de octubre de 1995 hasta el 24 de mayo de 2018, los tratamientos de datos personales estuvieron regulados en el derecho secundario de la Unión por 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[2].

[1] En adelante, “La Carta”.

[2] En adelante, “Directiva 95/46”

El 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esto8s datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[3], que entró en vigor el 25 de mayo de 2016 pero, en virtud de lo dispuesto por su art. 99, su aplicabilidad se aplazó hasta el 25 de mayo de 2018.

La base del ámbito territorial del RGPD está en su art. 3.1, que dispone que éste se aplica a los tratamientos que se realicen en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Una manera de reformular esta base territorial de aplicación del RGPD para simplificarla, sería afirmar que dicha norma se aplica a todo tratamiento de datos personales que esté relacionado con las actividades de un establecimiento[4] situado en el territorio de la Unión.

Las transferencias internacionales de datos personales son una especie concreta de la gran variedad de operaciones o tratamientos que se pueden realizar con los datos personales[5], al que el RGPD dedica todo un capítulo debido a un elemento distintivo que las hace especiales, al que nos referiremos más adelante dado que consideramos necesario detenernos antes sobre el significado del término *transferencias* cuando se

[3] En adelante, "RGPD".

[4] El legislador ha querido que el ámbito de aplicación territorial del RGPD sea particularmente extenso, a efectos de evitar que los interesados se vieran excluidos de su protección (Sent. TJUE de 13 de mayo de 2014 en el Asunto C-131/12, conocida como "Sentencia Google Spain", apartado 54). Por ello la jurisprudencia del TJUE ha interpretado el concepto de "Establecimiento" que utiliza el RGPD en este artículo de manera amplia y flexible, entendiendo como tal "el ejercicio efectivo y real de una actividad mediante una instalación estable", siendo indiferente la forma jurídica del mismo (considerando 19 de la Directiva 95/46). Por otra parte, el TJUE ha declarado en la Sentencia de 1 de octubre de 2015 en el asunto C-230/14 (conocida como "Weltimmo") que la concepción de establecimiento es flexible y no coincide necesariamente con el lugar de registro de una persona jurídica (párrafo 29) y que en determinadas ocasiones la presencia de un único representante puede bastar para constituir un 'establecimiento' (ibidem, párrafo 30). Ver también RIPOL CAROLLA, S: "VI. Aplicación territorial del Reglamento" En PIÑAR MAÑAS, J.L. (Dir.): Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad. 1ª Ed., Editorial Reus, Madrid 2016. Págs. 84-89. En SVANTESSON, D.J: *Article 4(1)(a) 'establishment of the controller' in EU data privacy law—time to rein in this expanding concept?" International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 210-221*, el autor presenta algunas opiniones contrarias a que las conclusiones del TJUE en la Sentencia Google Spain puedan aplicarse a otros operadores o responsables de tratamientos fuera de los motores de búsqueda.

[5] PIÑAR MAÑAS, J.L.: "XXV. Transferencias de datos personales a terceros países u organizaciones internacionales". En PIÑAR MANAS, J.L. (Dir.): Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad. 1ª Ed., Editorial Reus, Madrid 2016, pág. 428. El hecho de que sea una forma especial de tratamiento de datos personales implica que se le aplica en primer lugar toda la regulación del RGPD para los tratamientos y luego la regulación especial para las transferencias internacionales.

aplica a la protección de datos personales ya que, por un lado, ese concepto no está definido en las normas europeas[6] y, por otro, en este ámbito difiere del significado que adquiere en otros ámbitos como pueden ser el jurídico o el financiero.

Una *transferencia internacional de datos personales* implica cesión o envío, así como comunicación[7] hacia un destinatario titular de un establecimiento ubicado fuera de la Unión. Hasta aquí poca diferencia con los significados de esta expresión en otros ámbitos; mas una de las particularidades que adquiere cuando se refiere a los datos es que éstos pueden ser *transferidos* sin abandonar el territorio de la Unión o, incluso, sin haber estado nunca en él: Piénsese por ejemplo en un tratamiento que está relacionado con las actividades de un establecimiento en la Unión, pero las operaciones de éste las realiza exclusivamente otro establecimiento en un país tercero de la persona jurídica responsable; o los datos que están almacenados en la nube, en un servidor cuya verdadera localización se desconoce por razones competitivas[8]. Igualmente, pueden ser *transferidos* sin dejar de estar a disposición del remitente, si éste facilita el acceso al soporte de almacenamiento de los datos a una tercera persona[9]. Por otra parte, en los

---

[6] Al respecto: KUNER, C.; SVANTESSON, D.J.B. et al.: "The language of data privacy law (and how it differs from reality)." International Data Privacy Law. Vol. 6, nº 4 (2016): Pág. 259; PIÑAR MAÑAS, J.L.: "XXV. Transferencias…" cit., pp. 431-433.

[7] Cesión o comunicación de datos es "*… cualquier revelación o manifestación de datos a un tercero… una modalidad de tratamiento que… precisa de una base de legitimación propia, sea ésta el previo consentimiento del interesado, sea la existencia de algún título habilitante establecido por la Ley"*. NUÑEZ GARCÍA, L.: "XIX El encargado del tratamiento". En PIÑAR MANAS, J.L. (Dir.): Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad. 1ª Ed., Editorial Reus, Madrid 2016. Pág. 321.

[8] Son las conclusiones a que llega el TJUE en la sentencia Google Spain, según exponemos a continuación:

a) En la mencionada sentencia (apartado 43), el TJUE considera acreditado que tanto Google Search (www.google.com) como su versión española Google Spain (www.google.es) están gestionados por Google Inc., empresa matriz con establecimiento principal en Estados Unidos, desde servidores cuya ubicación se desconoce por razones competitivas (no habiéndose acreditado si están en un Estado miembro o en un país tercero).

b) Por ello el tratamiento de datos personales del cual es responsable Google Inc. y para el cual Google Spain promociona y vende publicidad en España (que es la forma de obtener rentabilidad de ese tratamiento) se realiza "*en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio de* (España)", expresión que remitía al derecho nacional aplicable según el art. 4.1.a de la Directiva 95/46, vigente al momento de dictarse la sentencia (apartados 55 a 57). Ya que sin la rentabilidad conseguida a través de Google Spain, el tratamiento no tendría sentido.

c) Con las afirmaciones precedentes el TJUE aclaró que el derecho de la Unión se aplica a los tratamientos de datos personales realizados por la matriz Google Inc que están relacionados con la publicidad que se gestiona desde las filiales europeas (ya que, aunque la sentencia se haya referido en exclusiva a la filial española, la doctrina que de ella emana se aplica a todas las filiales en territorio europeo).

[9] PIÑAR MAÑAS, J.L.: "XXV. Transferencias…" (cit.), pág. 433.

tratamientos de datos personales intervienen en muchas ocasiones ciertos medios tecnológicos (que pueden ser distintos para el almacenamiento y el procesamiento), personas o entidades que pueden estar ubicados en distintos lugares, países e incluso continentes y, en algunos casos, de ubicación desconocida tal como acabamos de comentar, por lo que sería difícil (cuando no imposible) determinar una ubicación o localización precisa para dichos datos.

Por todo ello, lo realmente significativo cuando nos referimos a las *transferencias internacionales de datos personales* es el hecho de que los datos, o el tratamiento al que están siendo sometidos, estén exclusivamente regidos por el derecho europeo o lo estén también por el derecho de un país tercero[10]. O, en otras palabras, que los datos, cuyo tratamiento estaba sometido al derecho europeo o de un estado miembro, merced a una transferencia ingresan al ámbito de vigencia del ordenamiento jurídico de un país tercero (en muchas ocasiones, sin dejar de estar sometidos también al derecho de la Unión) [11].

Y, debido a la imposibilidad de determinar la ubicación de los datos o el lugar de realización de su tratamiento, tanto los tratamientos a los que se aplica el derecho europeo en calidad de derecho de origen como las transferencias internacionales de los datos personales deben estar minuciosamente regulados, pues de lo contrario sería muy fácil eludir el nivel de protección y la responsabilidad de los agentes intervinientes.

I. LAS TRANSFERENCIAS INTERNACIONALES EN EL RGPD.

[10] Al referirnos a las transferencias internacionales de datos personales nos limitaremos a las realizadas hacia terceros países (que son países ubicados fuera de la Unión Europea o de los territorios donde se aplica el derecho de un Estado miembro) para simplificar, si bien el Capítulo V del RGPD se refiere también al envío de datos personales a organizaciones internacionales, a las que no se aplica el derecho de ningún estado sino sus propias normas.

[11] En KUNER, C.: "Extraterritoriality and regulation of international data transfers in EU data protection law." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 235-245, el autor expone una discusión sobre la supuesta extraterritorialidad de la regulación de las transferencias internacionales en el derecho europeo de protección de datos; sin embargo, en nuestra opinión, la verdadera extraterritorialidad del RGPD yace en el ámbito de aplicación territorial descrito en los dos apartados del art. 3 del Reglamento y no en la regulación de las transferencias.

El RGPD regula las transferencias internacionales de datos personales en el Capítulo V, artículos 44 a 50[12], en el primero de los cuales se advierte que sólo se podrán realizar bajo las condiciones y requisitos establecidos en este capítulo.

La primera condición establecida para que la transferencia de datos personales a un país tercero no implique una disminución de la protección que esos datos gozan en la Unión es que la Comisión haya adoptado una decisión por medio de la cual declara que el nivel de protección de los datos personales garantizado por el derecho del país receptor es adecuado[13]. Para adoptar esa decisión, la Comisión debe previamente evaluar ciertos aspectos (enumerados no taxativamente en el apartado 2 del artículo 45 RGPD) del derecho de ese país, de un determinado territorio o de un sector del mismo y, si al finalizar ese análisis, considera que ese derecho ofrece un nivel de protección de los datos personales "adecuado"[14], puede emitir una decisión expresándolo así, que permitirá que las transferencias internacionales de datos personales hacia ese país se puedan realizar sin ninguna otra exigencia.

A falta de decisión según lo indicado en el párrafo precedente, sólo se podrán transmitir datos personales hacia un país tercero o una organización internacional si el responsable o el encargado establecidos en la Unión ofrecen garantías adecuadas[15], que entre otros

---

[12] En esta investigación nos limitaremos a analizar los flujos de datos personales en los cuales tanto el emisor como el receptor sean personas privadas, dado que las transferencias en las cuales participan entes de derecho público tienen otras características cuyo análisis excede los cometidos de este artículo Por otra parte, las transferencias en las que interviene la Unión, sus órganos o autoridades están reguladas en otra norma: El Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento [CE] nº 45/2001 y la Decisión nº 1247/2002/CE, Capítulo V, arts. 46 a 50).

[13] Art. 45 RGPD.

[14] El TJUE ha considerado que "*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…*" (Sentencia del TJUE de 6 de octubre de 2015 en el asunto C-362/14, que en adelante llamaremos "Sentencia Schrems", apartado 73). En definitiva, por *nivel adecuado* debe entenderse un nivel *sustancialmente equivalente*, que no necesita ser idéntico al de la Unión.

[15] A pesar de que el art. 46.1 expresamente establece que, a falta de decisión de adecuación, las transferencias "*sólo*" podrán realizarse garantizadas con las medidas que explicamos en los párrafos siguientes, el art. 49 RGPD establece "Excepciones" a esa exigencia de garantías, que son: El consentimiento informado del interesado o un justificación legítima de la necesidad de la transferencia, tales como la ejecución o preparación de un contrato, razones importantes de interés público, el ejercicio o la defensa de derechos o intereses vitales del interesado. Adviértase que en todos estos casos la transferencia debe ser necesaria a esos fines y ello se debe poder demostrar (principio de responsabilidad proactiva).

requisitos deben mantener la responsabilidad de dichos agentes frente a incumplimientos en que incurra el receptor y asegurar a los interesados derechos exigibles y recursos administrativos y judiciales idóneos para hacerlos efectivos.

Las garantías que establece el RGPD pueden consistir en:

1. Normas corporativas vinculantes (arts. 46.2.b y 47 RGPD);
2. Cláusulas protección de datos, que se pueden subdividir en:
   a) Cláusulas contractuales tipo[16] aprobadas mediante una decisión de la Comisión (art. 46.2.c RGPD, que remite al procedimiento de examen establecido en el art. 93.2 del mismo Reglamento), o
   b) CCT adoptadas por una autoridad de protección de datos y posteriormente aprobadas por la Comisión (por el mismo procedimiento que las anteriores, art. 46.2.d RGPD); o
   c) Cláusulas específicas previamente autorizadas por una autoridad de control (art. 46.3.a RGPD);
3. Un código de conducta, aprobado en virtud de lo dispuesto por el art. 40 RGPD (art. 46.2.e RGPD).
4. Una certificación aprobada y otorgada según lo prescrito por el art. 42 RGPD (art. 46.2. f RGPD). Tanto la certificación como el código de conducta deben estar acompañadas por compromisos vinculantes y exigibles del responsable o del encargado del tratamiento.

II. DECISIONES DE LA COMISIÓN SOBRE EL NIVEL DE PROTECCIÓN DEL DERECHO ESTADOUNIDENSE Y JURISPRUDENCIA DEL TJUE AL RESPECTO.

En aplicación de las facultades que le otorga el art. 45.2 RGPD, la Comisión adoptó distintas decisiones declarando adecuada la protección otorgada por el derecho de distintos países, territorios y sectores[17].

[16] En adelante, "CCT".

[17] Que se pueden consultar en el apartado específico de la página web de la Comisión Europea, dentro de la sección dedicada a la protección de datos personales: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_es (en inglés, último acceso 22/12/2020).

De entre todas ellas nos enfocaremos en las que tenían por objeto los flujos de datos hacia los Estados Unidos por dos motivos: Por un lado, constituyen el destino más frecuente de las transferencias[18] y, por otro, porque las dos decisiones que afectaban a ese país tenían algunos aspectos que las diferenciaban del resto: La Comisión no se limitó a analizar el derecho norteamericano sino que, además, negoció con las autoridades de ese país la aprobación por parte de éstas de una serie de principios y compromisos que las empresas con sede en su territorio podrían obligarse a respetar por medio de la cumplimentación de un procedimiento que se llamó "autocertificación", ofreciendo así un nivel de protección de los datos personales que podría ser declarado adecuado mediante una Decisión de la Comisión.

Esas Decisiones eran la Decisión de la Comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los Principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América[19], que fue anulada por la Sentencia Schrems; y la Decisión de Ejecución (UE) 16/1250 de la Comisión, de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE.UU[20], que fue anulada por la Sentencia Schrems II.

En la primera de dichas sentencias el TJUE constata, entre otros hechos, las siguientes circunstancias:

1) Que ciertas normas estadounidenses sobre vigilancia que realiza la inteligencia para la seguridad y defensa[21] permitían a las autoridades y organismos dedicados a ello acceder a los datos transferidos desde la Unión y tratarlos de una forma "*que va más allá de lo que era estrictamente necesario y proporcionado para la*

[18] Según la normativa anterior al RGPD las transferencias internacionales de datos necesitaban de la autorización de las autoridades nacionales de protección de datos. Al momento de entrar éste en vigor la Agencia Española de Protección de Datos (AEPD) había otorgado 2.196 autorizaciones, de las que 966 eran hacia Estados Unidos (Memoria Anual de la AEPD de 2018 apartado 3.1.1. Transferencias Internacionales).

[19] En adelante, "Decisión Puerto Seguro".

[20] En adelante, "Escudo de Privacidad".

[21] Que en el derecho estadounidense tienen primacía sobre los principios de Puerto Seguro (apartado 86 Sent. Schrems).

protección de la seguridad nacional"[22], incompatible con la Directiva 95/46 y con los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea ya que "*una normativa… 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* (esa) *medida e impongan una reglas mínimas…*"[23] y que "*... 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…*"[24]

2) Que frente a esas injerencias de las autoridades norteamericanas, el interesado con residencia en la Unión Europea carecía de vías administrativas o judiciales efectivas para hacer valer los principios de Puerto Seguro y los derechos que éstos les reconocían, es decir que ante una violación de su derecho fundamental a la protección de datos personales carecía de acceso a la tutela judicial efectiva, lo que es incompatible con el art. 47 de la Carta[25].

Sin perjuicio de esas constataciones, el TJUE no declara la nulidad de la Decisión Puerto Seguro en virtud de la falta de un nivel adecuado de protección de los datos personales en el derecho estadounidense; sino por los siguientes motivos:

1) El art. 25.6 de la Directiva 95/46 habilita a la Comisión para hacer constar que un tercer país, "*a la vista de su legislación interna o de sus compromisos internacionales*"[26] garantiza un nivel de protección adecuado; ahora bien, la Decisión de Puerto Seguro no hace constar que Estados Unidos, por su legislación interna o por los compromisos internacionales asumidos, garantice un nivel de protección adecuado; sino que en su art. 1 declara que dicho nivel está garantizado por los principios de Puerto Seguro aplicados de conformidad con el resto de medidas publicadas por el gobierno de los Estados Unidos, lo que

[22] Sent. Screms, párrafo 90.

[23] Ibid., párr. 91.

[24] Ibid., párr. 92.

[25] Párrafos 86 a 95 de la Sentencia Schrems. En estos apartados el TJUE se remite a la Sentencia de 8 de abril de 2014 en los asuntos acumulados C-293/12 y C-594/12, conocida como "Sentencia Digital Rights Ireland", en cuyos párrafos 51 a 54 el Tribunal establece que las excepciones y restricciones a la protección del derecho a la intimidad y los datos personales se deben establecer "*… sin sobrepasar los límites de lo estrictamente necesario*".

[26] Art. 25.6 de la Directiva 95/46, citado textualmente en el párrafo 81 de la Sent. Schrems.

claramente se diferencia de la "legislación o compromisos internacionales asumidos" por ese país[27]. Por todo ello el TJUE declara que "*... 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"*[28].

2) El art. 3 de la Decisión Puerto Seguro limitaba los casos en los que las autoridades nacionales de protección de datos personales podían suspender los flujos de datos personales hacia una entidad que hubiera asumido los Principios de Puerto Seguro, de forma incompatible con el art. 28 de la Directiva 95/46, que establecía que las autoridades nacionales debían "*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…*"[29]. En virtud de ello, el TJUE halla que dicho artículo excede los poderes conferidos a la Comisión por el art. 25.6 de la Directiva 95/46, por lo que corresponde declarar su invalidez[30].

La segunda decisión adoptada por la Comisión, el Escudo de Privacidad, por su parte, contenía algunas mejoras respecto a la anterior; de entre las cuales cabe destacar:

1) Tanto en sus considerandos como en su articulado y anexos se analizaban detenidamente distintas normas norteamericanas relacionadas con los derechos a la privacidad y a la protección de datos personales, algunas de ellas relacionadas con la vigilancia realizada por la inteligencia, la seguridad y defensa nacionales;
2) Su art. 1 declaraba que los Estados Unidos garantizan un nivel adecuado de protección de datos personales;
3) No se limitaban las facultades de las autoridades nacionales para suspender los flujos de datos hacia empresas que se hubieran autocertificado de acuerdo con los principios del Escudo de Privacidad;

[27] Sent. Schrems, párrafos 79 a 81 y 97.

[28] Ibid., párr. 98.

[29] Ibid., párr. 99.

[30] Ibid., párrafos 102 y 105.

4) Creaba un defensor del pueblo en el ámbito del Escudo de la Privacidad[31], que atendería las reclamaciones presentadas por las autoridades nacionales de control a un organismo intermediario creado ad hoc para ello (ni los interesados ni las autoridades de protección de datos tendrían acceso directo a esta autoridad), relativas al acceso de autoridades de seguridad y defensa a sus datos personales. Una vez aceptada la solicitud (podría ser rechazada por motivos de forma), su función se limitaría a gestionarla tomando contacto con la autoridad u organismo contra el que estuviera dirigida la queja y evaluar si el tratamiento denunciado respetaba la regulación aplicable. Luego de realizadas esas gestiones, el Defensor del Pueblo informaría al organismo ad hoc que ya se había encargado de su solicitud, sin posibilidad de dar información concreta sobre el tratamiento (ni siquiera podría informar si dicho tratamiento existía o no) ni sobre las consecuencias de sus gestiones. Además, el DP no sería independiente sino que debería rendir cuentas al Secretario de Estado[32].

En la Sentencia Schrems II el TJUE analiza algunas normas estadounidenses a las que se hace referencia en la decisión Escudo de Privacidad[33], con el objetivo de determinar si dichas normas reconocían a los interesados "*derechos efectivos y exigibles"* tal como lo exige el art. 45.2 a) del RGPD[34]. Concluye que aquéllas permiten la injerencia de los servicios de inteligencia en los derechos fundamentales protegidos por la Carta, en una forma incompatible con ésta. En concreto, vulneran el derecho a la privacidad (art. 7 de la Carta), el de protección de datos personales (art. 8 de la Carta) y la tutela judicial efectiva (art. 47). Agrega que, si bien existen normas que establecen algunas exigencias vinculantes para las autoridades que llevaran a cabo la inteligencia exterior, no se podía

[3131] En adelante, "DP".

[32] Decisión Escudo de la Privacidad, Anexo A: "La figura del Defensor del Pueblo en el ámbito del Escudo de la privacidad UE-EE. UU. con relación a la inteligencia de señales." Cabe aclarar que, con respecto a incumplimientos por parte de las entidades autocertificadas sí existían recursos administrativos, judiciales y arbitrales efectivos que se describían en la decisión y sus anexos.

[33] Por ejemplo, la Foreign Intelligence Surveillance Act (Ley de Vigilancia de Inteligencia Exterior, "FISA", citada en el considerando 78 y, entre otros pasajes, en la nota 66 del considerando 70), su art.702, referido en el considerando 81, en el que también se mencionan dos programas de inteligencia estadounidenses: Los programas PRISM y Upstream, sobre los que hay alguna información más en la nota 89 del considerando 82; la Executive Order 12333 y la Presidential Policy Directiv 28, citadas en el Considerando 68. De la sentencia podemos colegir que el análisis que realiza el TJUE es indirecto, es decir lo realiza a través de las referencias, citas y descripción de los contenidos de esas normas que contenía la Decisión Escudo de la Privacidad.

[34] Sent. Schrems II, párrafo 177.

afirmar que tales exigencias fueran verdaderos límites a las injerencias mencionadas[35] y, además, no establecen recursos ni garantías efectivas para las personas no nacionales de los Estados Unidos que se pudieran ver afectadas por las mismas[36]. En ese sentido, declara que la figura del DP no garantizaba un control jurisdiccional efectivo para los interesados que se sintieran afectados por las injerencias de las autoridades u organismos en sus datos personales[37], vulnerando así el art. 45.2.a) del RGPD y el art. 47 de la Carta[38], no sólo por la limitación de sus funciones[39] sino también por no ser una figura independiente[40].

Como colofón el TJUE declara inválida la Decisión del Escudo de la Privacidad por vulnerar los artículos 7, 8 y 47 de la Carta, lo que la hace incompatible con el art. 45.1 del RGPD[41].

VARDANYAN y STEHLIK[42], en una crítica a la Sentencia Schrems II sugieren que en ella el objetivo de priorizar la protección de los derechos fundamentales se ha realizado mediante un completo desprecio hacia el factor económico representado por los obstáculos interpuestos a las transferencias de datos personales hacia los Estados Unidos, que pueden ocasionar un declive de la competitividad de las empresas europeas.

III. LAS CLÁUSULAS CONTRACTUALES TIPO

[35] Tal como lo requiere el art. 52, apartado 1, segunda frase de la Carta (Sent. Schrems II, párraf. 185).

[36] Ibid., párr. 180 y 181. De la interpretación *a sensu contrario* de estas afirmaciones se desprende que para los nacionales de los Estados Unidos sí existen garantías efectivas para exigir la aplicación de los límites o exigencias a que están sometidas las actividades de inteligencia.

[37] Ibidem, párrafos 187 y 190.

[38] Ibidem, párr. 191.

[39] Ibidem, párr. 196.

[40] Ibidem, párr. 195. En este párrafo el TJUE destaca, entre las afirmaciones de la Decisión del Escudo de Privacidad, que en ella se describe al Defensor del Pueblo como "independiente de los servicios de inteligencia" pero que "informará directamente al secretario de Estado, que garantizará que aquel desempeñe sus funciones de manera objetiva y sin ninguna influencia indebida…" VARDANYAN y STEHLIK ("Schrems II: Will it really increase the level of privacy protection against mass surveillance? Bratislava Law Review, 4(2), pág. 118) resaltan la insistencia del TJUE en órganos judiciales independientes como garantes de la privacidad; no obstante, en los párrafos de la Sent. Schrems II que se refieren a los recursos efectivos para hacer valer derechos exigibles, el TJUE se refiere también a las acciones administrativas (párrafo 189: "*La existencia de posibilidades efectivas de* ***acciones administrativas*** *y judiciales en el país tercero que se trate tiene una especial importancia en el contexto de una transferencia de datos personales a ese país tercero…*").

[41] Ibidem, apartados 198 a 201.

[42] Op. Cit., pág. 120.

Ante la anulación de cada una de las decisiones sobre la adecuación del nivel de protección de los datos personales del derecho estadounidense, las herramientas que más han utilizado los exportadores que antes se amparaban en ellas para garantizar las transferencias hacia ese país han sido las CCT, que salvo algunos casos[43], también deben ser aprobadas por una decisión de la Comisión.

Así, en utilización de las facultades establecidas en el art. 45.2.c) y 45.2.d) del RGPD[44] la Comisión ha aprobado distintos grupos de cláusulas contractuales tipo mediante las Decisiones que presentamos a continuación, agrupadas según los sujetos intervinientes en las transferencias:

1) Transferencias realizadas por un responsable establecido en la Unión, hacia un responsable establecido en un país tercero: Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE y la Decisión 2004/915/CE de 27 de diciembre de 2004 por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países.
2) Transferencias realizadas por un responsable establecido en la Unión, hacia un encargado establecido en un país tercero: Decisión 2010/87/UE de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo[45].

[43] Las denominadas *cláusulas contractuales ad hoc*, que no están aprobadas por la Comisión sino por las autoridades de protección de datos para transferencias concretas, es decir que sólo se pueden utilizar por el responsable o encargado que ha solicitado su aprobación, para la o las series de transferencias para las que se han autorizado (art. 46.3.a del RGPD).

[44] En realidad, las Decisiones que mencionamos a continuación no se adoptaron bajo la vigencia del RGPD sino bajo la de su antecesora, la Directiva 95 /46 (arts. 25 y 26) pero al ser derogada ésta por el RGPD, dichas decisiones mantienen su vigencia y validez en virtud de lo establecido por los arts. 46.5 y 94 apartados 1. y 2. de éste.

[45] En adelante, "Decisión 2010/87". Anteriormente la Comisión había adoptado la Decisión 2002/16/CE, de 27 de diciembre de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, que fue derogada por la Decisión 2010/87.

Por ello el TJUE, en la Sentencia Schrems II, tuvo la posibilidad de pronunciarse asimismo sobre la validez de la Decisión 2010/87[46] dado que la reclamación que dio origen al procedimiento fue presentada ante la autoridad irlandesa de protección de datos en contra de transferencias hacia Estados Unidos que se efectuaron en el período que transcurrió entre la anulación de la Decisión Puerto Seguro y la aprobación del Escudo de la Privacidad y estaban garantizadas mediante cláusulas contractuales tipo aprobadas por dicha decisión. Bien que cuando el órgano judicial irlandés remitió la cuestión prejudicial esta última decisión ya estaba en vigor, lo que le dio la posibilidad de introducir algunas preguntas sobre ella que dieron lugar a su declaración de nulidad.

Adelantaremos que el TJUE, luego de valorar el contenido de la Decisión 1020/87 y relacionarlo con el capítulo del RGPD dedicado a las transferencias internacionales, se decanta por la validez de esta Decisión, si bien determina la necesidad de complementarlas con otras medidas cuyo análisis resumimos a continuación.

El TJUE recuerda que las CCT, como medida para garantizar las transferencias internacionales, se ubican en el Capítulo V del RGPD, presidido por el art. 44 cuyo contenido establece como principio general de las transferencias (aplicable por lo tanto al resto de artículos de este Capítulo) la necesidad de "*asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado*", independientemente de cuál sea la herramienta utilizada para garantizarlo[47].

Y para asegurar la continuidad de ese nivel de protección los interesados deben contar con derechos exigibles y acciones legales efectivas[48], lo que las partes en la transferencia deben garantizar mediante las estipulaciones contractuales adoptadas entre ellos si han elegido este medio de garantía. Ahora bien, uno de los aspectos más destacables de esta sentencia es la obligación que el TJUE pone a cargo del responsable[49], de determinar si los interesados disponen de esos derechos y acciones en

---

[46] Párr. 149 de la Sent. Schrems II, que es consecuencia del análisis de la Decisión que se realiza en los párrafos precedentes.

[47] Sent. Schrems II, párrafos 92 y 96.

[48] Ibidem, párr. 103.

[49] Aunque no se menciona en la Sentencia, esta obligación es una manifestación del principio de responsabilidad proactiva del responsable (art. 5.2. del RGPD) tal como expresa el Comité Europeo de Protección de Datos (CEPD) en los apartados 1.3 y 1.4 de sus "Recommendations 01/2020 on measures that supplement transfer tools to ensure complicance with the EU level of protection of personal data", adoptadas el 10 de noviembre de 2020 como consecuencia de la Sentencia Schrems II,

relación con el posible acceso a los datos por parte de las autoridades públicas del país del destinatario: para ello debe realizar, en colaboración con el importador de los datos si fuera necesario, un análisis de las disposiciones pertinentes del ordenamiento jurídico de éste y, en particular, de los elementos mencionados en el art. 45.2 del RGPD[50]. Si, una vez analizado ese ordenamiento jurídico, las partes llegan a la conclusión de que las cláusulas[51] pueden no ser respetadas, están obligadas a adoptar otras medidas de garantía que conserven el nivel de protección de datos de la Unión[52].

Pero es aún más destacable la advertencia que hace el TJUE en el párrafo 135 de la Sentencia Schrems II: "*Si el responsable o el encargado de tratamiento establecidos en la Unión no pueden adoptar medidas adicionales suficientes para garantizar esa protección, estos…están obligados a suspender o poner fin a la transferencia… En particular, eso es lo que ocurre cuando el Derecho de ese país tercero impone al destinatario de una transferencia de datos personales procedentes de la Unión obligaciones que son contrarias a las referidas cláusulas y que, por tanto, pueden poner en entredicho la garantía contractual de un nivel de protección adecuado contra el acceso de las autoridades públicas del mencionado país tercero a esos datos*".

Aunque la obligación de analizar el derecho del país receptor no es exclusiva del responsable del tratamiento ya que las cláusulas aprobadas por la Decisión 2010/87 la ponen también a cargo del destinatario bajo un enunciado distinto[53]: Al momento de asumir las cláusulas, el destinatario debe certificar que no tiene motivos para creer que la legislación que le es de aplicación le impida cumplir las obligaciones que ha asumido a través de éstas y, posteriormente, si cambian las circunstancias y surgen esos motivos,

---

disponibles en el original en inglés en la dirección: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en. Esta sentencia sí establece, en los párrafos 140 y 141, que esa obligación surge de la interpretación combinada de las cláusulas 4.a); 5.a) y 5.b) del anexo de la Decisión 2010/87 "*… interpretada*(s) *a la luz de las disposiciones del RGPD y de la Carta*" (apartado 140 *in fine*).

[50] Ibidem, párrafos 104 y 105. Análisis que el CEPD interpreta que debe hacerse caso por caso, para cada serie de transferencias (Recomendaciones 01/2020, apartado 46).

[51] Las exigencias que el TJUE impone a las partes en las transferencias garantizadas mediante cláusulas contractuales se aplican también a las normas corporativas vinculantes (CEPD: Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 – Comisaria de Protección de Datos vs Facebook Irlanda y Maximilan Schrems. Adoptadas el 23 de julio de 2020, Pregunta nº 6. Traducción al castellano disponible en la página web de la AEPD: https://www.aepd.es/sites/default/files/2020-08/faqs-sentencia-SCHREMS-II-es.pdf. Último acceso 22/12/2020). Ello implica que las conclusiones de esta sentencia sobre la Decisión 2010/87 se aplican también a las restantes Decisiones sobre CCT.

[52] Sent. Schrems II, párr. 134.

[53] Ibidem, párr. 139, que hace referencia a las cláusulas 5.a) y 5.d) de la Decisión 2010/87.

debe notificarlo al remitente. En caso de que, recibida esa notificación, el responsable o encargado exportadores decidan no suspender ni poner fin a la o las transferencias, deben poner la notificación en conocimiento de la autoridad de control de datos competente para que obre en consecuencia[54].

Las medidas adicionales que deben adoptar el responsable o el encargado establecidos en la Unión en esos casos en que las cláusulas no sean garantía suficiente para la continuidad del nivel de protección de los datos personales pueden ser cláusulas complementarias o cualquier otra medida que el responsable o el encargado consideren suficiente[55].

El CEPD[56] desarrolla los pasos que el exportador de datos debe seguir para evaluar si las cláusulas son garantía suficiente y, si no lo son, especifica que las medidas adicionales a adoptar pueden ser "*... de naturaleza contractual, técnica u organizacional.*"[57]; si bien aclara[58] que cuando el derecho de un país tercero autorice a las autoridades públicas para acceder a los datos de forma incompatible con las obligaciones asumidas en las cláusulas, en muchos casos las medidas contractuales y organizacionales no serán suficientes para evitarlo, por lo que deben estar complementadas por medidas técnicas que creen obstáculos para impedir que las autoridades públicas accedan a los datos o para que su acceso sea infructuoso. Por ello, en nuestra opinión, revisten especial interés la propuesta de que los datos se transfieran seudonimizados o anonimizados.

De la lectura de las Recomendaciones 01/2020 se desprende que, a criterio del CEPD, hay dos maneras de transferir datos personales hacia receptores en Estados Unidos:

1) Garantizándolas mediante cláusulas contractuales o normas corporativas vinculantes, con la adopción de medidas complementarias (especialmente técnicas) que el exportador considere suficientes;
2) Mediante alguna de las excepciones del art. 49 RGPD, siempre que se cumplan todas las condiciones dispuestas en este artículo. Pero el CEPD advierte que

[54] Ibidem, párr. 145.

[55] Ibidem, párrafos 132 y 133.

[56] Recomendaciones 01/2020, apartados 2.3 y 2.4.

[57] Traducción libre de la autora, del inglés original: "*... In principle, supplementary measures may have a contractual, technical or organisational nature...*" Párrafo 47 de las Recomendaciones 01/2020.

[58] Recomendaciones 01/2020, párrafo 48.

estas excepciones son de naturaleza excepcional, deben ser interpretadas de forma restrictiva y sólo se aplican a actividades de tratamientos que son ocasionales y no repetitivas[59].

El CEPD va más allá de la decisión del TJUE en la Sent. Schrems II, agregando que si no se pueden hallar medidas suficientes para garantizar que los datos gozarán de una protección similar a la que les ofrece el derecho europeo, además de interrumpir (o no iniciar, en su caso) las transferencias, las copias de los datos que se habían transferido se deben devolver al remitente o ser destruidas por el importador[60].

IV. ACTUACIÓN Y FACULTADES DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS ANTE LAS DECISIONES DE LA COMISIÓN.

Finalmente, en la sentencia Schrems el TJUE analiza las posibilidades de actuación que tendrían las autoridades de protección de datos si consideran que un país respecto del cual exista una decisión de adecuación no ofrece un nivel adecuado de protección; llegando a la conclusión de que impedir las transferencias hacia ese país constituiría un incumplimiento de dicha decisión y, por lo tanto, la única opción que tienen es acudir al órgano judicial competente para instar una cuestión prejudicial ante el TJUE y que éste se pronuncie acerca de la validez de la mentada decisión.

En la sentencia Schrems II analiza igualmente si las autoridades de protección de datos podrían impedir transferencias internacionales garantizadas por CCT aprobadas por una Decisión de la Comisión. Concluyendo que, si ante una transferencia garantizada por un conjunto de cláusulas contractuales tipo autorizadas por una decisión de la Comisión, la autoridad de control competente considera que las partes no las están cumpliendo o el derecho del país receptor hace que su cumplimiento sea imposible, puede suspender o prohibir las transferencias sin que ello signifique un incumplimiento de la decisión de la Comisión[61].

---

[59] Ibidem, párrafo 25.

[60] Recomendaciones 01/2020, apartado 52 y Preguntas frecuentes… pregunta nº 7.

[61] Sent. Schrems, apartado 52 y Sent. Schrems II, apartados 113 146 y 156.

CONCLUSIONES

El legislador europeo ha autorizado a la Comisión a *evaluar* el derecho de un país tercero y, en cierto sentido, *aprobar* un determinado aspecto de ese derecho (el nivel de protección de los datos personales) a fin de otorgarle una ventaja, cual es la de que se puedan realizar transferencias hacia receptores en ese país sin ningún otro requisito.

En las dos ocasiones en que la Comisión ha hecho uso de esa autorización para facilitar las transferencias de datos hacia Estados Unidos, el hecho de que haya necesitado negociar con sus autoridades un conjunto de disposiciones, compromisos y mecanismos que complementen el derecho de ese país a efectos de declarar que sólo conservarían el nivel de protección de los datos las transferencias que fueran enviadas a las empresas autocertificadas es una muestra evidente de que el derecho de ese país no ofrecía un nivel de protección adecuado, evidencia que el TJUE pone de manifiesto con claridad meridiana en sus sentencias Schrems y Schrems II.

Ahora bien, no es el hecho de que las autoridades puedan acceder a los datos personales transferidos lo que el TJUE censura, sino que dichos accesos, que son injerencias en el derecho fundamental a la protección de datos personales, no cuenten con reglas claras que le impongan límites razonables, así como la falta de control por parte de organismos administrativos independientes y de tutela judicial frente a esas injerencias.

Así, si la finalidad de la habilitación a la Comisión para evaluar el derecho de un país tercero es la conservación de un alto nivel de protección de los datos personales cuando éstos entren en el ámbito de vigencia del ordenamiento jurídico de ese país. Por ello, según el RGPD, esa evaluación debe garantizar que el derecho de ese país tercero cuenta con dos elementos básicos: Derechos exigibles y garantías efectivas. Elementos a los que el TJUE agrega: Limitaciones razonables a las excepciones a la protección, órganos administrativos independientes y tutela judicial.

Además, la sentencia Schrems II extiende esa facultad de evaluar el nivel de protección de los datos personales de los países terceros a toda persona o entidad que pretenda exportar tales datos; con dos diferencias: 1) Para dichos responsables o encargados la evaluación del derecho de ese país tercero al que deseen enviar los datos no constituye una *facultad* sino una *obligación*; 2) Las conclusiones a que llegue cada persona o

entidad sólo afectarán a las transferencias que ella pretenda realizar; mientras que la aprobación de la Comisión afectará a toda transferencia que se quiera realizar hacia ese país desde un Estado miembro.

Paralelamente, también otorga a las autoridades nacionales de protección de datos personales una base legal para impedir las exportaciones hacia los países que a su criterio no ofrezcan un nivel adecuado de protección (siempre que no exista una Decisión de adecuación de la Comisión respecto de ese país), incluso cuando dichas transferencias estén garantizadas mediante un conjunto de cláusulas aprobadas por una decisión de la Comisión. Si bien es cierto que, en este caso, sólo se pueden impedir por hechos externos a las cláusulas (y, por lo tanto, a la Decisión) tales como un posible incumplimiento de sus obligaciones por parte del importador o por el posible acceso de las autoridades públicas del país receptor de una forma incompatible con las cláusulas o con el derecho de la Unión.

En cuanto a las transferencias de datos personales hacia los Estados Unidos han quedado en una situación muy delicada, en nuestra opinión debido a que la concepción norteamericana del derecho a la privacidad y su relación con el derecho a la seguridad es evidentemente diferente de la concepción de estos dos derechos y de la ponderación entre ellos que se hace en la Unión. Por ello los exportadores de datos hacia ese país deberán examinar exhaustivamente sus transferencias a fin de elegir cuidadosamente las medidas más efectivas para garantizarlas, dando prioridad a las medidas técnicas que impidan o hagan infructuoso el acceso de las autoridades a los datos, tales como la anonimización, la seudonimización o garantías similares.

Finalmente, reflexionando sobre la colisión entre los factores jurídico y económico que puede emanar de esta sentencia, entendemos que no es la función del TJUE dar prioridad al segundo sobre el primero, sino interpretar la voluntad del legislador manifestada a través de las normas de derecho vigente, al que está sujeto tanto el mismo Tribunal como la Comisión, que sí tiene la función de velar por la buena marcha de la economía de la Unión y de la competitividad de sus empresas pero, nuevamente, también dentro de los límites y facultades marcados por el derecho vigente.

BIBLIOGRAFÍA

1. BOEHME-NEßLER, V.: "Privacy: a matter of democracy. Why democracy needs privacy and data protection." International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 222-229.
2. CERDA SILVA, A.: "El 'nivel adecuado de protección' para las transferencias internacionales de datos personales desde la Unión Europea" ["The "Adequate Level of Protection" for International Personal Data Transfer from the European Union"]." Revista de Derecho. Nº 36 (2011): Pp. 327-356.
3. DE HERT, P.; CZERNIAWSKI, M.: "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context." International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 230-243.
4. FLORIDI, L: *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press, Oxford, 2014.
5. HILDEBRANDT, M.: "Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace." University of Toronto Law Journal. Vol. 63, nº 2 (2013): Pp. 196-224. doi:10.3138/utlj.1119.
6. HON, W.K.; HÖRNLE, J. y MILLARD, C.: "Data protection jurisdiction and cloud computing - when are cloud users and providers subject to EU data protection law? The cloud of unknowing." International Review of Law, Computers & Technology. Vol. 26, nº 2-3 (2012): Pp. 129-164. doi:10.1080/13600869.2012.698843.
7. KUNER, C.; CATE, F.H. *et al.*: "The (data privacy) law hasn't even checked in when technology takes off." International Data Privacy Law. Vol. 4, nº 3 (2014): Pp. 175-176. doi:10.1093/idpl/ipu013.
8. KUNER, C.: "Extraterritoriality and regulation of international data transfers in EU data protection law." International Data Privacy Law. Vol. 5, nº 4 (Nov 2015, 2015): Pp. 235-245.
9. KUNER, C.; SVANTESSON, D.J.B. *et al.*: "The language of data privacy law (and how it differs from reality)." International Data Privacy Law. Vol. 6, nº 4 (2016): Pp. 259-260.

10. LESIEUR, F.: "Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy." International Data Privacy Law. Vol. 2, nº 2 (2012): Pp. 93-104.

11. MARTÍNEZ DE PISÓN, J.: "Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo". Derechos y Libertades. Nº 37 (2017): Pp. 51-84.

12. MC CULLAGH, K.: "Cross-Border Data Protection: Applicable Law and Territorial Powers of National Data Protection Supervisors." Scripted. Vol. 13, nº 1 (Mayo 2016, 2016): Pp. 95-100.

13. MIGUEL ASENSIO, P.A.: "Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea." Revista Española de Derecho Internacional. Vol. 69, nº 1 (2017): Pp. 75-108.

14. NUÑEZ GARCÍA, L.: "XIX El encargado del tratamiento". En PIÑAR MANAS, J.L. (Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. 1ª Ed., Editorial Reus, Madrid 2016. Pp. 321-333.

15. PIÑAR MAÑAS, J.L (Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. 1ª Ed., Editorial Reus, Madrid 2016.

16. PIÑAR MAÑAS, J.L.: "XXV. Transferencias de datos personales a terceros países u organizaciones internacionales". En PIÑAR MANAS, J.L. (Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. 1ª Ed., Editorial Reus, Madrid 2016. Pp. 427 a 460.

17. REBOLLO DELGADO, L.: *El derecho fundamental a la intimidad.* 2ª act ed. Ed. Dykinson, Madrid: 2005.

18. REBOLLO DELGADO, L.: *Protección de datos en Europa. Origen, evolución y regulación actual.* Ed. Dykinson, Madrid: 2018.

19. REBOLLO DELGADO, L.: *Vida privada y protección de datos en la Unión Europea.* Ed. Dykinson, Madrid: 2008.

20. RIPOLL CARULLA, S.: "Aplicación territorial del Reglamento". En PIÑAR MANAS, J.L. (Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. 1ª Ed., Editorial Reus, Madrid 2016. Pp. 77-96.

21. RUBENS, J.; MORSE, E.: "Survey of the Law of Cyberspace: Introduction." Business lawyer. Vol. 69, nº 1 (2013): Pp. 183-187.

22. RUIZ MIGUEL, C.: "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico." Revista de Derecho Comunitario Europeo. Vol. 7, nº 14 (2003): Pp. 7-43.

23. SANCHO VILLA, D.: *Transferencia internacional de datos personales.* Ed. Agencia española de protección de datos, Madrid: 2003.

24. SERRANO PÉREZ, M.M.: "El derecho fundamental a la protección de datos. Su contenido esencial". Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas, 2005, Issue 1, pp.245-265

25. SVANTESSON, D.J.: "A "layered approach" to the extraterritoriality of data privacy laws." International Data Privacy Law. Vol. 3, nº 4 (2013): Pp. 278-286.

26. SVANTESSON, D.J.: "Article 4(1)(a) 'establishment of the controller' in EU data privacy law—time to rein in this expanding concept?" International Data Privacy Law. Vol. 6, nº 3 (2016): Pp. 210-221.

27. SVANTESSON, D.J.B.; Institutet för rättsinformatik (IRI) *et al.*: "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation." International Data Privacy Law. Vol. 5, nº 4 (2015): Pp. 226-234. doi:10.1093/idpl/ipv024.

28. VARDANYAN, L. y STEHLIK, V.: "Schrems II: Will it really increase the level of privacy protection against mass surveillance? Bratislava Law Review, 4(2). https://doi.org/10.46282/blr.2020.4.2.215. Pp. 111-128

BREVE GLOSARIO

DATOS PERSONALES: Son los datos que pueden dar información sobre una persona física identificada o que se pueda identificar, de forma directa o indirecta, a través de esos datos o de la combinación de éstos con otra información.

ENCARGADO: Según el art. 4.8) RGPD, es la persona, organismo o entidad que realiza los tratamientos por cuenta del responsable, que "*... se caracteriza por encontrarse sometido, precisamente, a las decisiones del* (responsable)[62]

EXPORTADOR, EMISOR o REMITENTE: Persona o entidad que comunica, envía o comparte los datos con otra entidad establecida en un país tercero, o permite el acceso de ésta a los datos.

IMPORTADOR, RECEPTOR o DESTINATARIO: Persona o entidad establecida en un país tercero que recibe los datos o accede a ellos. El exportador y el importador son las partes en una transferencia internacional de datos.

INTERESADO: La persona sobre la cual los datos dan información o a la que los datos identifican.

RESPONSABLE: Es la persona, organismo o entidad que determina los fines y medios del tratamiento.

TRATAMIENTO DE DATOS PERSONALES: Toda operación que se realiza con este tipo de datos, tales como: recogida, registro, organización, estructuración, conservación, adaptación, procesamiento, utilización, comunicación, difusión, compartición o habilitación de acceso, etc.

[62] NUÑEZ GARCÍA, L.: "XIX El encargado del tratamiento". En PIÑAR MANAS, J.L. (Dir.): *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*. 1ª Ed., Editorial Reus, Madrid 2016. Pág. 324.