Facultad de Ciencias Sociales y Jurídicas

Grado en Derecho

Universidad de Jaén

Facultad de Ciencias Sociales y Jurídicas

Trabajo Fin de Grado

TRANSFERENCIA INTERNACIONAL DE DATOS; RÉGIMEN JURÍDICO.

Alumna: Tatiana Hermoso Moya

Julio, 2020

RESUMEN

El presente estudio nos muestra la vigente legislación en materia de protección de datos y su ineludible evolución donde las instituciones europeas han jugado un papel de vital importancia a la hora de subsanar las controversias surgidas. Se analizan sentencias clave que han desafiado la legislación europea que sirven de precedentes para la implantación de una unificada y proactiva legislación. El estudio de algunos preceptos del Reglamento General de Protección de Datos que atañe al Derecho internacional privado nos trasmite una elevada seguridad en esta materia, pero la vertiginosa evolución tecnológica y los defectos de contenido analizados por algunos expertos auguran una posible futura modificación en la legislación.

PALABRAS CLAVE

Reglamento General de Protección de Datos, protección de datos, Unión Europea, tratamiento de datos.

ABSTRACT

This study shows us the current legislation on data protection and its inescapable evolution where the European institutions have played a vital role in settling disputes that have arisen. Key judgments that have challenged European legislation that serve as precedents for the implementation of a unified and proactive legislation are analyzed. The study of some precepts of the General Data Protection Regulation that concerns private international law transmits a high degree of security in this matter, but the dizzying technological evolution and the content defects analyzed by some experts predict a possible future modification in the legislation.

KEYWORDS

General Data Protection Regulation, data protection, European Union, data processing.

INDICE

Abreviatura	Significado
Art.	Artículo
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CEDH	Convenio Europeo para la Protección de los Derechos Humanos
DPC	Comisario Irlandés de Protección de Datos
EEE	Espacio Económico Europeo
EM	Estado Miembro
EE.UU	Estados Unidos
LOPD	Ley Orgánica de Protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos y de Garantía de Derechos Digitales
NSA	Agencia de Seguridad Nacional de los Estados Unidos
PNR	Registro de nombres de pasajeros para la prevención de delitos terroristas y delitos graves.
PRIMS	Programa de Vigilancia Masiva de los Estados Unidos
RGPD	Reglamento General de Protección de Datos
SEPD	Supervisor Europeo de Protección de Datos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TFTP	Programa de Seguimiento de la Financiación del Terrorismo
TJCE	Tribunal Judicial de las Comunidades Europeas
TJUE	Tribunal de Justicia de la Unión Europea
TL	Tratado de Lisboa
TFUE	Tratado de Funcionamiento de la Unión Europea

1. INTRODUCCION.

La globalización y la vertiginosa evolución tecnológica han propiciado un devenir constante de las legislaciones en materia de protección de datos. La capacidad de almacenaje y de intercambio de datos se ha acentuado de forma significativa en consecuencia de una utilización sin precedentes de datos personales por medio de autoridades publicas y empresas privadas en el ejercicio de su actividad. Los avances tecnológicos han contribuido en la renovación del sistema económico y social teniendo que reforzar su nivel de protección ante terceros países.

La rigidez de las normas para abarcar un problema presente, que en potencia está sometido a una futura permuta, la convierte en una posterior norma obsoleta. Es por ello que, las instituciones europeas que competen esta materia, han ido interiorizando esa necesidad de cambio y se ha trasformado en una responsabilidad para determinar a corto plazo la implantación de una legislación versátil.

El estudio versa sobre la vigente legislación en materia de protección de datos y su ineludible evolución, por ello, se analizará la derogación de la Directiva 96/46/CE[1] y la posterior implantación del Reglamento (UE) 2016/679[2]. A través de este análisis, profundizaremos sobre el derecho de protección de datos personales con el fin de obtener una perspectiva general de las vicisitudes en materia de protección y tratamiento de datos que ha supuesto este cambio de normativa. Nos adentraremos en aspectos como su evolución, legislación vigente, ámbito de aplicación, competencia judicial internacional, entre otros aspectos relevantes de la protección de datos. El estudio revela un valor indiscutible al Reglamento ya que encauza una regulación uniforme de protección de datos a nivel europeo favoreciendo a una protección necesaria y eminente. Sin embargo, el análisis de determinados preceptos augura modificaciones futuras en el Reglamento.

[1] 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. Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050.

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (Reglamento general de protección de datos). Diario Oficial nº L 119 de 4.5.2016, p. 1/88.

Las trasferencias internacionales de datos personales ha sido un tema de gran relevancia que ha desafiado la legislación de la Unión Europea en constantes conflictos judiciales debido a la incierta legalidad de determinadas normas instauradas en la Unión Europea (en adelante, U.E.). Una muestra de ello, son las controversias presentadas ante la justicia europea como la sentencia del Tribunal de Justicia de la Unión Europea (en adelante, STJUE) de nulidad de la Decisión 2004/535/CE[3], la resolución sobre la suspensión del acuerdo del Programa de seguimiento de la Financiación del Terrorismo (en adelante, TFTP)[4] y la STJUE de nulidad de la Directiva 95/46/CE (en adelante, caso Schrems).

La STJUE de la Gran Sala sobre el asunto C-362/14, el conocido caso Schrems, deroga 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 conferida por los principios de puerto seguro, declarando la nula garantía de protección de datos que esta ofrecía en la trasferencia de datos personales con Estados Unidos (en adelante, EE.UU.).

El caso Schrems abre las puertas al nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo 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 adelante, RGPD) tras la anulación de la Directiva 95/46/CE, es por ello, que será objeto de estudio para comprender las insuficiencias legislativas que ofrecía la UE a los Estados miembros.

Por último, se tratará el vigente Reglamento (UE) 2016/679 que servirá como modelo comparativo con las deficiencias legislativas de la Directiva y proporcionará un nuevo enfoque en el tratamiento de datos personales. En definitiva, la entrada en vigor del Reglamento a supuesto una transición de un modelo reactivo a uno proactivo.

[3] Tribunal de Justicia de la Unión Europea. C-317/04 y C-318/04.
[4] La Resolución del Parlamento Europeo, de 23 de octubre de 2013, que esclareció la vigilancia masiva de la NSA y su acceso a los datos SWIFT de trasmisión de datos bancarios sin cumplir con el acuerdo TFTP. Por tanto, solicitó en sus resoluciones, tras su ineficaz aplicación, la suspensión del acuerdo TFTP.

2. LA PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA.

El Parlamento Europeo ha llevado a cabo un refuerzo en la tutela de los derechos humanos siendo la protección de los datos personales y el respeto de la vida privada derechos fundamentales a proteger, consagrados en la Carta de los Derechos Fundamentales de la UE[5] (en adelante, CDFUE).

La trasferencia internacional de datos personales ha de comprenderse desde la doble posición del Derecho Comunitario Europeo y el Derecho Internacional. La definición de Tratamiento de datos se localiza en el Informe explicativo del Convenio 108+[6], artículo 14 definiéndola como aquellos datos personales que se difunden o se dejan al servicio de un destinatario sometido a la jurisdicción de otro Estado u organización internacional.

El concepto más renovado de la protección de datos lo hallamos en el art. 4.1 del Reglamento General de Protección de Datos (en adelante, RGPD): *"Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"*

Conforme a la doctrina, la transferencia internacional de datos corresponderá presentar una serie de elementos[7]:

1. Datos de carácter personal; como cualquier tipo de información bien sea numérica, alfabética, etc. relativo a personas físicas determinables. En definitiva, que permita ser *"identificable toda persona cuya identidad pueda determinarse, directa o indirectamente"*[8]

[5] La protección de datos personales. Fichas temáticas sobre la Unión Europea. Parlamento Europeo (2020). Consultado el 17 de mayo de 2020, en https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

[6] Convenio nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos trasfronterizos de datos. BOE-A-1985-23447

[7] Vid. Ortega Giménez, A., *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, AEPD, Madrid (2015), pp. 23, y *Transferencias internacionales de datos de carácter personal ilícitas*, Cizur Menor, Aranzadi (2017), p. 31.

[8] Artículo 4.1) del RGPD.

2. La trasmisión de los datos de carácter personal tienen alusión tanto a los tratados de carácter automatizado como a los tratados de carácter no automatizado.

3. La transferencia internacional de datos se consuma con el fin de formalizar un tratamiento de datos de carácter particular por parte del destinatario, siendo esta por medio de cesión a otro responsable o como prestación de un servicio, es decir, un encargado de tratamiento.

4. La transacción física efectiva de los datos de carácter personal, de una parte del Espacio Económico Europeo (EEE) a otro Estado u Organización Internacional.

5. El lugar de destino de los datos de carácter personal ha de hallarse en una región externa al EEE o de las partes no contratantes.

6. La existencia de la transferencia internacional de datos personales será cierta cuando establezca una cesión o comunicación de datos o cuando tenga por objeto la ejecución de un tratamiento de datos por parte del responsable mediante un encargo de tratamiento.

El principio general de trasferencia internacional de datos regulado en diferentes normativas de aplicación[9] decretan que solo se podrán realizar transferencias internacionales de datos a un tercer país u organización internacional si: 1) cumple con las obligaciones referentes al tratamiento reguladas en la normativa aplicable; 2) asegura las garantías necesarias en el momento de realizar la transferencia internacional. Por consiguiente, cuando un responsable proyecta transferir datos personales a un tercer Estado, región u organización internacional tiene que certificar que cumple con los elementos obligatorios y que si se trasfiere a otros proveedores debe de certificar también que estos amparen todas las garantías necesarias, no solo bastaría con afirmar que es segura.

La trasferencia internacional de datos, según norma general, será autorizada a través de una decisión de adecuación que constate que ese país u organización internacional asume poseer un nivel de protección adecuado sin la exigencia de autorización de cualquier Autoridad de Supervisión. La decisión de adecuación es un acto jurídico ejecutado por la Comisión Europea y regulado por el RGPD y el artículo 288 del TFUE. Cabe hacer mención, a la STJUE Schrems, con la que se construyen los requisitos básicos para la adecuación de la protección de datos de la legislación europea.

[9] Artículos 44 del RGPD, 36 de la Directiva 206/680 y 14 del Convenio 108+.

Por otro lado, el Grupo de trabajo del artículo 29 (posteriormente denominado Comité Europeo de Protección de Datos) publicó el WP254 en febrero de 2018, un reajuste del WP12, que establece unos requisitos respecto a la consideración como "adecuado" para el nivel de protección de un Estado, el cual era de 1998[10]. El nuevo WP aparece para desarrollar las exigencias reguladas en el artículo 45 del RGPD. La adecuación se obtiene mediante los derechos asignados a los afectados, las obligaciones dadas a los garantes del tratamiento, el cumplimiento de los derechos por parte del respaldo del organismo y, en mayor parte, un sistema que avale la efectividad de la legislación en vigor.

2.1. Marco institucional.

2.1.1. Tratado de Lisboa.

La legislación referente a la protección de datos en el espacio de libertad, seguridad y justicia previa al Tratado de Lisboa[11] (en adelante, TL) estaba regulada por la protección de datos con fines privados y comerciales con aplicación del método comunitario y por la protección de datos con fines de aplicación de la ley con toma de decisiones intergubernamental. Con la llegada del Tratado de Lisboa se consolida una base para el desarrollo de un sistema mas eficaz de protección de datos y anuncia para el Parlamento Europeo nuevas competencias confiándole el cargo de colegislador.

2.1.2. Disposiciones estratégicas en el espacio de libertad, seguridad y justicia.

El Consejo Europeo instauró en 2009, en materia de libertad, seguridad y justicia para la etapa 2010-2014, el programa de Estocolmo[12]. Las disposiciones estratégicas de la sistematización legislativa en el espacio de libertad, seguridad y justicia fueron definidas en sus conclusiones de 2014 conforme al art. 68 del TFUE[13]. El objeto principal fue la mejora de protección de datos personales.

---

[10] WP12, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" adoptado por el Working Part el 24 de julio de 1998.

[11] Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea que entró en vigor el 1 de diciembre de 2009. Diario Oficial nº C 306 de 17.12.2007, p. 1/271.

[12] Programa de Estocolmo - Una Europa abierta y segura que sirva y proteja al ciudadano del Consejo Europeo, de 4 de mayo de 2010. Diario Oficial nº C 115 /1.

[13] Art. 68 TFUE: *"El Consejo Europeo definirá las orientaciones estratégicas de la programación legislativa y operativa en el espacio de libertad, seguridad y justicia."*

2.2. Instrumentos legislativos.

2.2.1. Carta de los Derechos Fundamentales de la Unión Europea.

La Carta de los Derechos Fundamentales de la UE en sus artículos 7 y 8 regulan la protección de los datos de carácter personal y el respeto de la vida privada siendo estos derechos fundamentales independientes.

2.2.2. Consejo de Europa.

a. Convenio n.º 108 de 1981.

La primera legislación internacional vinculante para la defensa y protección de la protección de datos donde se presentaba el tratamiento automatizado de datos fue el Convenio n.º108 del Consejo de Europa. Tuvo como objeto avalar el respeto de los derechos y libertades fundamentales en relación al tratamiento automatizado de los datos de carácter personal como dicta su art.1[14]. La modificación del Convenio a través de un Protocolo amplió su ámbito de aplicación, mejoró su eficacia y su nivel de protección.

b. Convenio Europeo de Derechos Humanos (CEDH), de 1950.

El Convenio Europeo de Derechos Humanos conforme a lo referente en materia de protección de datos se destaca su art. 8 sobre el derecho al respeto de la vida privada y familiar: "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".*

[14] Convenio nº 108. Art. 1: *"El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona".*

2.3. Actos legislativos vigentes de la Unión en materia de protección de datos.

2.3.1. Reglamento general de protección de datos (RGPD).

La entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE en 2018, brotó ante la necesidad de mejora de protección en la Unión Europea derivada de las violaciones de privacidad y de datos personales cometidas por Estados externos a la Unión. Del mismo modo, se presentó un marco mas claro para las empresas que operaban dentro y fuera de la unión dotándolo de más coherencia y eficacia. Las mejoras se pueden resumir en la entrada de un consentimiento claro y expreso dotado de un derecho a recibir información sobre dicho consentimiento, un derecho al olvido[15], la posibilidad de trasferir datos de un proveedor de servicios a otro proveedor entre otras modificaciones. Cabe destacar, la imposición de medidas correctoras en caso de infracción de las normas.

2.3.2. Directiva sobre protección de datos en el ámbito penal.

La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, también entró en vigor en 2018. Las autoridades competentes son las encomendadas para efectuar el cumplimiento de esta Directiva que tutela el derecho fundamental a la protección de datos. Esta directiva actúa como garante de que los datos personales de sospechosos de infracciones sean adecuadamente protegidos. También coopera transfronterizamente frente a la delincuencia y el terrorismo.

[15] Reglamento (UE) 2016/679. Art. 17.: "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad [...] al responsable del tratamiento."

2.3.3. Directiva de privacidad y comunicaciones electrónicas.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas fue modificada por la Directiva 2009/136/CE, de 25 de noviembre de 2009. Actualmente, existe una propuesta de Reglamento[16] que derogaría la Directiva 2002/58/CE.

2.3.4. Reglamento referente al tratamiento de los datos personales por instituciones y organismos de la Unión.

En 2018, entró en vigor el Reglamento (UE) 2018/1725[17] por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

2.4. Acuerdos internacionales para la trasferencia de datos en la Unión Europea.

2.4.1. Decisiones de adecuación en la trasferencia comercial de datos.

Conforme a lo estipulado en el el artículo 45 del RGPD, se otorga a la Comisión la decisión de nivel de adecuación a los países no pertenecientes a la Unión fundamentándose en la legislación nacional y en los compromisos internacionales acogidos

2.4.2. Acuerdo marco UE-EE. UU.

El Parlamento aprobó el acuerdo entre Estados Unidos (en adelante, EE.UU) y la UE sobre la protección de datos personales asegurándose de prevenir, investigar, detectar y enjuiciar las infracciones penales, conocido como "Acuerdo marco". El acuerdo tiene como fin garantizar un elevado nivel de protección de los datos personales que se trasmiten transatlánticamente en

[16] Reglamento del Parlamento Europeo y del Consejo, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Diario Oficial nº L-2016-80807.
[17] 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. Diario Oficial nº L 295/39.

el marco de la cooperación a efectos de aplicación ley, principalmente para la lucha contra el terrorismo y la delincuencia organizada.

2.4.3. Acuerdos UE-EE. UU., UE-Australia y UE-Canadá sobre el registro de nombres de los pasajeros (PNR).

Los acuerdos bilaterales firmados por la UE sobre el registro de nombres de los pasajeros ayudan a las autoridades encargadas a combatir el terrorismo y la delincuencia grave gracias al acceso de datos personales de pasajeros en sus reservas de vuelos guardadas por las compañías aéreas.

2.4.4. Programa UE-EE. UU. de Seguimiento de la Financiación del Terrorismo (TFTP)[18]

Con el objeto de la persecución de la financiación del terrorismo la UE y los EE.UU firmaron un acuerdo bilateral sobre el tratamiento y la transferencia de datos de mensajería financiera.

2.5. Autoridades de la Unión de supervisión de datos.

El Supervisor Europeo de Protección de Datos (en adelante, SEPD)[19] tiene la competencia de avalar que las instituciones y órganos de la UE desempeñen las obligaciones destinadas a la protección de datos. Es una autoridad independiente el cual cumple las funciones de consulta, asesoramiento, control y cooperación.

El Comité Europeo de Protección de Datos (inicialmente, el Grupo de Trabajo Artículo 29) es un organismo de personalidad jurídica cuya estructura está compuesta por representantes de la UE de autoridades nacionales competente sobre esta materia, la Comisión y el Supervisor Europeo de Protección de Datos. Su función es asesorar y supervisar conforme a lo estipulado den el RGPD y de la Directiva sobre protección de datos en el ámbito penal.

[18] U.S Department of the Treasury. Terrorist Finance Tracking Program (TFTP). Disponible on line: https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp
[19] Supervisor Europeo de Protección de Datos. Unión Europea. Disponible on line: https://edps.europa.eu/

3. LA DEFICIENCIA DE CONTENIDO DE LA DIRECTIVA 95/46/CE.

Previamente, al estudio de la Directiva 95/46/CE y su derogación, se ha de resaltar su espíritu moderador y armonizador hacia la tutela de los derechos de tratamiento de datos personales. Así mismo, se ha de considerar esta directiva como un elemento promotor del progreso de la economía y del mercado puesto que crea una legislación que salvaguarda los derechos de los estados miembros reforzando y aproximando las legislaciones nacionales y cerciorándose de que esta no disminuye, sino que aumenta la protección de este derecho en los estados miembros de la Unión Europea.

El amparo al derecho de protección de datos personales fue calando en la Unión como una necesidad que precisaba urgentemente establecer iniciativas como la Propuesta de Directiva de 1990[20]. Esta propuesta colisionaba con el contraste de diferentes enfoques nacionales sobre el tratamiento de datos personales que podían conllevar a un Estado miembro poner inconvenientes a la libre circulación de datos acogiéndose a una falta de protección en el Estado de procedencia o destino o inclusive conllevar a un engaño de la competencia entre los agentes económicos privados según las limitaciones establecidas en su país.

En cambio, la Directiva 95/46/CE, aparece para enmendar la problemática planteada con la aplicación del art. 1 *"Los Estados miembros garantizarán la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales."* Del mismo modo, en su segundo párrafo prohíbe la restricción de la libre circulación de datos personales entre los Estados miembros fundamentándose con la protección adoptada en el primer párrafo.

El contraste con la propuesta de la Directiva mencionada con anterioridad es que en ella se protegía únicamente el derecho de la intimidad de las personas[21] a diferencia de la Directiva 95/46/CE donde se amplía la protección hacia las libertades y los derechos fundamentales. También existe una clara diferencia con el objeto del Convenio 108 del Consejo de Europa, la

[20] Herrán Ortiz, A. I. (2002). *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*. Dykinson, Madrid, pp. 388.

[21] BOE-A-1979-24010. CEDH. Cit., art. 8:. *"Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia."*

falta de una reseña de garantía frente al "tratamiento automatizado", limitación implantada en el Convenio.

La negociación y posterior implantación de la Directiva tuvo muchas objeciones por parte de los Estados miembros ya que se hacía mención en esas réplicas al Convenio del Consejo de Europa, el cual ya trataba el amparo de los individuos frente al tratamiento automatizado de sus datos personales, fue por ello, que se terminó adoptando la introducción en el texto, el apartado 2 del art. 1 de la Directiva como objeto de la misma. Partiendo de esta base, obtenemos que la Directiva no ha de tratarse como un medio de protección de los individuos sino como un propósito de imposibilitar los inconvenientes a la libre circulación de la información personal en la U.E.

La Directiva introduce una serie de definiciones en su artículo 2 que delimitan el ámbito material de aplicación: *"A efectos de la presente Directiva, se entenderá por: a) «datos personales»: toda información sobre una persona física identificada o determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social; b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción; c) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;"*.

Se puede constatar que la definición de datos personales es deliberadamente amplia con el propósito de englobar toda la información de la persona. Para que indudablemente el tratamiento de un dato se halle en el ámbito de aplicación, corresponderá recoger dos circunstancias: la primera, ha de referirse a un dato personal concerniente a la persona física; la segunda, ha de tratarse de una persona identificable o identificada. Cabe destacar que no es

objeto de la Directiva la figura de personas jurídica, así lo dicta el considerando 24 de la Directiva.[22]

Referente al ámbito de aplicación territorial la Directiva 95/46/CE ha sido de aplicación a los tratamientos de datos por compañías instituidas en el área de la U.E, o que a pesar de no estar instauradas en el a U.E manipulasen los datos personales a través de medios automatizados no situados en el área del Estado miembro (con excepción de que el medio se utilizase con fin de tránsito), correspondiendo otorgar en esta circunstancia un representante instaurado en el territorio U.E.

Desde una perspectiva general, la Directiva cumplía con los requisitos necesarios para ser garante del derecho de protección de datos personales. Sin embargo, la presencia de algunos asuntos que concernían a esta legislación en los Tribunales Europeos, puso en punto de mira a la Directiva. Las deficiencias en materia de protección de derechos fundamentales como la tutela efectiva y el derecho a la vida privada e inclusive la supervisión de las autoridades competentes promulgó una derogación de la Directiva en la STJUE del Caso Schrems.

3.1 Sentencia del Tribunal de Justicia de la Unión Europea. La nulidad de la Directiva 95/46/CE.

El litigio iniciado por el estudiante austriaco de Derecho, Maximiliam Schrems, contra "Facebook Ireland Ltd.", la filial internacional de Facebook y la empresa matriz "Facebook Inc." en 2013, tras las revelaciones de Edward Snowden[23] sobre Estados Unidos y su programa de vigilancia masiva PRIMS, supuso una trasformación en el panorama de la trasferencia internacional de datos personales.

El afamado "Caso Schrems" fundamentó una vulneración hacia los datos personales de los consumidores acometiendo contra una legislación que no avalaba un grado adecuado de protección sobre sus derechos. Paralelamente, perpetuó la curiosidad mediática y a posteriori, la vigilancia sobre los movimientos internacionales de datos que llevaban a cabo los Tribunales

[22] Directiva 95/46/CE. Considerando nº24.: *"Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva."*

[23] Edward Snowden. Ex empleado de la CIA que destapó los programas de vigilancia masiva ilegal en Estados Unidos.

europeos e internacionales. Asimismo, forzó el replanteamiento de la eficiencia sobre bases jurídicas que hasta el momento modulaban su regulación.

La trasmisión ilícita de datos sospechada por Maximiliam Schrems da lugar a la queja[24] presentada ante el Comisario Irlandés de Protección de Datos (en adelante, DPC) en 2013 que acusaba a Facebook Iireland ltd. de ser un medio de control y de trasmisión de los datos de sus usuarios a EE.UU. Una vez transferidos, "Facebook inc.", adscrito al "Acuerdo de Puerto Seguro UE – EE.UU"[25], procesaba la información recibida y las cedía de forma ilegítima.

Según Maximiliam Schrems no había una razón obligatoria para trasferir sus datos personales a los EE.UU haciendo hincapié en que sus datos podrían conservarse dentro de la UE / EEE. En su queja trasmite que el periódico British Guardian publicó documentos de la Agencia de Seguridad Nacional de los Estados Unidos (en adelante, NSA)[26] que verificaban que "Facebook Inc" estaba enviando los datos de usuarios a la NSA por motivos de espionaje, seguridad nacional y otros asuntos. Facebook aparece documentado como un "acceso masivo" cuyos datos son utilizados sin necesidad de causa justificable bajo el sistema llamado "PRISM" desde el 3 de junio de 2009 siendo esta una participación voluntaria de "Facebook Inc", junto con otras empresas, en este sistema.

Maximiliam Schrems alega la claridad del hecho de que "Facebook Ireland Ltd" ha subcontratado el procesamiento de sus datos a "Facebook Inc" y la transmisión de sus datos a servidores de los EE.UU. Al igual que la existencia de una causa probable para creer que "Facebook Inc" está otorgando a la NSA acceso masivo a sus servidores. Aclara que las declaraciones que ha realizado "Facebook Inc" sobre estas afirmaciones[27] son conforme a las leyes de los EE.UU y han de considerarlas no admisibles puesto que "Facebook Inc" está obligado por las órdenes de mordaza (Gag Orders) prohibiéndoles decir la verdad sobre dicho procesamiento e inclusive el deber de falsear sobre este asunto.

[24] Schrems, M (2013). Complaint against Facebook Ireland Ltd – 23 PRISM.
[25] Decisión. nº 2000/520/CE, comisión de las comunidades europeas, de 26 de julio de 2000, 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. Diario Oficial nº L 215/7.
[26] Macaskill, E y Dance, G (2013) "NSA files: Decoded."Disponible on line: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2
[27] Terdiman, D (2013) "Zuckerberg touts Facebook's mobile strength, says US 'blew it' on NSA." Disponible on line: https://www.cnet.com/news/zuckerberg-touts-facebooks-mobile-strength-says-us-blew-it-on-nsa/

Por lo tanto, pide al DPC que aclare los hechos y comprueben si los informes de “The Guardian” son falsos o sustancialmente inexactos sobre "Facebook Ireland Ltd". De la misma forma, le ruega que realice el mismo procedimiento con todas las quejas anteriores contra "Facebook Ireland Ltd"[28] haciéndoles recibir posteriormente el resultado conforme a sus derechos estipulados en el Art. 6 del Convenio Europeo para la Protección de los Derechos Humanos (en adelante, CEDH) y la ley irlandesa.

Tras una exposición de motivos, Maximiliam Schrems, argumenta legalmente todo lo detallado con anterioridad exponiendo que "Facebook Inc" es el procesador o subprocesador que trata los datos en nombre de "Facebook Ireland Ltd" según refleja los términos de uso en “Facebook.com”. Por consiguiente, "Facebook Ireland Ltd" está sujeto a Ley irlandesa de Protección de Datos (DPA) y la Directiva 95/46/CE. También destacó que en el asunto “SWIFT” el Grupo de Trabajo del Artículo 29[29] sostuvo que el uso masivo de datos comerciales con fines de investigación es un incumplimiento de los principios de propósito y de limitación. En consecuencia, en caso de operar los datos con fines de espionaje se ha de considerar este argumento para el caso de "Facebook Ireland Ltd".

Por lo tanto, dicho uso por parte de "Facebook Ireland Ltd" o sus subprocesadores vulneran el artículo 6.1.b. de la Directiva 95/46/CE[30] y la Sección 2, 1.c.ii. de la DPA. Maximiliam Schrems, concluye alegando que el procesamiento de datos personales del caso “SWIFT” parecen eludir las estructuras y los acuerdos internacionales existentes. Por tanto, "Facebook Ireland Ltd" no podría justificar el escenario con la regulación de los EE.UU, si se emplearan los argumentos de la decisión "SWIFT".

Sobre la transferencia de datos personales a los EE.UU, Schrems manifiesta que "Facebook Ireland Ltd " realiza una trasmisión de datos sin un "nivel adecuado de protección". Conforme a la regulación del art. 25 de la Directiva 95/46[31] solo está permitido si los derechos

[28] Quejas contra Facebook Ireland Limited (2011). Disponible on line: http://www.europe-v-facebook.org/ES/Quejas/quejas.html

[29] Grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales.

[30]Directiva 95/46/CE, cit., art. 6.1.b: “Los Estados miembros dispondrán que los datos personales sean recogidos con fines determinados, explicativos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible al tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas.”

[31] Directiva 95/46/CE, cit., art. 25.: “Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su

fundamentales y el derecho a la protección de datos de los interesados disfrutan de protección adecuada en el tercer país. Sin embargo, "Facebook Inc" está ligado al "Puerto Seguro" y con ello autocertifica que se adhiere a ciertos principios de protección de datos.

Dos principios que tienen que garantizar son los principios de aviso y elección, en otros términos, hablamos del consentimiento e información adecuada a los interesados en caso de transmisión de sus datos personales. Es por ello que esta queja exhibe la nula posibilidad de cumplir ambos principios en el reenvío de datos a la NSA al no ser que concurra la excepción de "seguridad nacional" contemplada en el cuarto párrafo del anexo 1 de la decisión "Safe harbor"[32]. Es por ello, que solicita al DPC que investigue si Facebook Inc" está enviando sus datos a la NSA por seguridad nacional, y si está en línea con las excepciones de "Safe Harbor", o si en caso contrario está cooperando de forma voluntaria, que verifiquen su ilegalidad.

Para fundamentar y ocasionar un estudio detallado de la protección de los datos personales conforme a las leyes establecidas, Schrems, cuestiona la redacción de la Decisión de la Comisión Europea sobre la adecuación del "Puerto Seguro" de el 26 de Julio de 2000. Considera que las excepciones podrían ser un "comodín" para que los EE.UU. limitara la aplicación de la decisión "Safe Harbor" a su merced. Esclarece que la excepción "seguridad nacional"[33] no queda definida o limitada al igual que tampoco incluye ninguna limitación que permita equilibrar estas excepciones con los derechos fundamentales de los interesados.

Tal interpretación del "Puerto Seguro" de ninguna manera podría estar en línea con el artículo 25 de la Directiva 95/46 /CE[34], al igual que estaría en contra del considerado artículo 10 de la

transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado."

[32] Decisión. nº 2000/520/CE, comisión de las comunidades europeas, de 26 de julio de 2000, 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). "La adhesión a estos principios puede limitarse: a) cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley."

[33] Decisión. nº 2000/520/CE cit. Anexo 1, cuarto párrafo: "La adhesión a estos principios puede limitarse: a) cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley."

[34] Unión Europea. Directiva. 95/46 /CE. Art. 25: "Principios. 1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado."

Directiva 95/46 /CE[35] y quebrantaría también el artículo 8 del CEDH[36]. Concluye con la problemática de la decisión de la Comisión Europea sobre el "puerto seguro" debido a las modificaciones masivas realizadas en la legislación estadounidense tras los ataques terroristas del 11 de septiembre de 2001 ya que se introdujeron nuevas leyes que difícilmente cumplían con las ideas europeas de los derechos humanos y el estado de derecho. Esta protección constitucional de los derechos humanos queda exenta a los ciudadanos de la UE debido a que EE.UU sigue la idea de "derechos civiles" (ciudadanos estadounidenses) en lugar de "derechos humanos". Este enfoque proporciona la visión de que una "apropiación masiva" de los datos personales de los ciudadanos de la UE no estaría cubierta por la legislación estadounidense.

Tras su fundamentación exigió al DPC que se cerciorase de que la Decisión de "Puerto Seguro" se interpretase de acuerdo con la Directiva 95/46/CE y los derechos fundamentales. Su recomendación, en caso de que fuera necesario, fue obtener inclusive una resolución preliminar por el Tribunal Judicial de las Comunidades Europeas (TJCE). El DPC impugnó la queja, por tanto, Schrems presentó una solicitud de revisión judicial en el Tribunal Superior de Irlanda por la inacción del DPC irlandés, que fue conferida.

El Sr. Justice Hogan (Juez del Tribunal Superior Irlandés), a fecha de 18 de junio de 2014, prorrogó el proceso a la dilación de una referencia al Tribunal de Justicia de la Unión Europea (TJUE). Expuso que, en materia de privacidad, la ley irlandesa fue suprimida por la ley europea y lanzó la propuesta de si se debería de reevaluar las directivas con la ulterior entrada en vigor del Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. *"Protección de datos de carácter personal: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos*

[35] Directiva. 95/46 /CE. Cit., Art. 10.: "Información en caso de obtención de datos recabados del propio interesado. Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, […] en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado."

[36] Convenio para la protección de los derechos humanos y las libertades fundamentales. 4 de noviembre de 1950, cit,. Art. 8.: "Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

El 24 de marzo de 2015 se celebró una audiencia por parte del Tribunal de Justicia de la Unión y el 23 de septiembre de 2015 se publicaron las conclusiones del Abogado General Sr. Yves Bot (asunto C-362/14*).* Dichas conclusiones cuentan con 237 puntos que termina reafirmando las premisas del Sr. Schrems, es por ello, que informa que*:*

> *"El artículo 28 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos, leído a la luz de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, debe interpretarse en el sentido de que la existencia de una Decisión adoptada por la Comisión Europea sobre la base del artículo 25, apartado 6, de la Directiva 95/46 no tiene por efecto impedir que una autoridad de control nacional investigue una denuncia en la que se alega que un país tercero no garantiza un nivel de protección adecuado de los datos de carácter personal y, en su caso, suspenda la transferencia de dichos datos. La Decisión 2000/520/CE 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, es nula.". (p.35)*

En fecha 6 de octubre de 2015, hace público su pronunciamiento, declarando la invalidez de la Decisión de la Comisión, de fecha 26 de julio de 2000, basándose en una serie de fundamentos jurídicos, los cuales serán objeto de comentario en las siguientes líneas de redacción.

El 6 de octubre de 2015, la sentencia del Tribunal de Justicia de la Unión Europea declaró la invalidez de la Decisión de la Comisión de 26 de julio de 2000 (2000/520/CE) basándose en diferentes aspectos jurídicos. Corroboró la potestad de inspeccionar y supervisar las transferencias de datos entre los EE. UU y la UE de las autoridades nacionales en virtud del artículo 28.1 de la Directiva 95/46/CE *"Los estados miembros dispondrán que una o mas autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva."*

Por ende, la cuestión a valorar residía en si existía un impedimento por parte de la Decisión de la Comisión para que una autoridad de control, como en este caso el DPC, pudiese inspeccionar la petición de un individuo con el objeto de confirmar si una trasferencia de datos personales desde el Estado Miembro hacia un tercer Estado cumplía con los requerimientos determinados por las Directivas. El Tribunal al respecto expuso que, aunque la Comisión adoptase una Decisión la cual presume la adecuada protección de los datos personales trasferidos, las autoridades nacionales tenían la competencia para indagar y examinar todas las solicitudes que pudiesen ser casos de vulnerabilidad de protección.

Por otro lado, en materia de Derechos fundamentales, el TJUE constató que el criterio para abordar la situación de vulneración de datos personales residía en la vulneración en sí de los derechos fundamentales, en concreto la protección de derecho a la vida privada. El Tribunal apreció que el nivel de protección que debía de ofrecer un tercer Estado tendría que equipararse a la protección que otorgaba la UE, es decir, una protección equivalente.

El TJUE considera que vulnera el derecho a la vida privada la normativa que consiente a las autoridades públicas acceder de carácter generalizado al contenido de las comunicaciones haciendo referencia al caso de los programas de vigilancia masiva divulgados por Snowden sin adentrarse en un fundamento probatorio *"…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 publicas 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"*[37].

De análoga manera, se consideró que se violó el contenido fundamental del derecho a la tutela judicial efectiva siendo esta inherente al Estado de derecho[38]:

[37] TJUE, Schrems, cit., 93.

[38] Puerto, M. I., y Sferrazza Taibi, P. (2017). "La sentencia Schrems del Tribunal de Justicia de la Unión Europea: Un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional." *Revista Derecho Del Estado*, (40), 209-236.

> *"El derecho interno norteamericano no contemplaba recursos judiciales eficaces para que los ciudadanos europeos pudiesen alegar una vulneración de sus derechos fundamentales en relación con sus datos personales, siendo que a 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. Por lo demás, la aplicación del derecho comunitario no puede impedir el ejercicio de la tutela judicial efectiva, que en materia de datos personales se concreta acudiendo a las autoridades nacionales de control." (*p.209)

Cabe destacar de la sentencia, la mención referente a la seguridad nacional frente a la amenaza terrorista que se establecía como un fin legítimo. En este caso, el TFUE, consideró que los programas ejecutados por los EE.UU no proporcionaba ninguna protección designada a limitar la injerencia en la privacidad. *"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"*.[39]

Conclusivamente, el TJUE invalidó el acuerdo del Puerto Seguro y afianzó la facultad de las autoridades nacionales en materia de protección de datos, ya adquirida en la anterior jurisprudencia, pero de manera que fortalecía el papel de guardianes de los derechos de privacidad y trasferencia de datos personales.

Este agresivo impacto de la deficiente e insatisfactoria Directiva 95/46/CE no solo a afectado en el ámbito de la seguridad nacional, sino que ha tenido gran repercusión en el ámbito del comercio internacional debido a su fin meramente comercial. Por consiguiente, ha sido ineludible, en el trascurso del tiempo, distinguir los efectos producidos en casos claramente de seguridad nacional, otros concernientes a intereses legítimos y otros relativos a las relaciones comerciales.

[39] TJUE. Schrems, cit., 88.

La Directiva no incluía únicamente a empresas estadounidenses ni si quiera se debe de considerar un asunto exclusivo de internet, el hecho del caso Scrhems y la vinculación con Facebook es un caso meramente circunstancial. Esta problemática afecta a la pluralidad del tejido comercial de la Unión Europea. Diferentes empresas utilizan recursos ubicados en EE.UU o bien se valen de proveedores europeos que emplean tales recursos de EE.UU para almacenar y tratar datos personales. Como hemos tratado en la sentencia analizada, estos proveedores prestan sus servicios debido a su adhesión al acuerdo del Puerto seguro. Tras su nulidad, estos proveedores tuvieron que tomar medidas que han sido de riesgo a nivel económico.

Articular, desarticular y volver a establecer un sistema de transferencias internacionales ha supuesto unos elevados costes para responsables y encargados del tratamiento de datos. De análoga manera, supuso una merma en los ingresos de diversas empresas debido a una escasa capacidad de competencia para la búsqueda y acceso al nuevo sistema de trasferencia internacional de datos personales. Todo ello, ocasionó un gran daño colateral: el enfriamiento con las relaciones comerciales, principalmente con un país de gran poder e influencia.

4. EL REGLAMENTO (UE) 2016/679.

El Reglamento General de Protección de Datos adopta medios y garantías al nuevo contexto social fortaleciendo y mejorando la eficacia en la protección de los individuos y atribuyendo renovadas obligaciones para las empresas. Este nuevo contexto normativo no impone una renuncia al modelo de protección instaurado por la Directiva 95/46/CE ni tampoco deshace la jurisprudencia consolidada por el TJUE. Por ello, su considerando segundo tiene como cimiento la permanencia de los principios fundamentales del derecho a la protección de datos. Su fin es dotar de coherencia y uniformidad una norma de aplicación proporcionando un correcto desarrollo económico y una mayor seguridad jurídica y practica[40]

Tanto el Reglamento como la Directiva comparten ciertos preceptos como es el caso del concepto de dato personal (art. 2.a Directiva y 4.1 RGPD), el objeto de las mismas, el concepto de tratamiento (art. 2.b Directiva y art. 4.2 RGPD) y el ámbito de aplicación material (art. 3 de la Directiva y 2 del RGPD).

Sin embargo, el nuevo Reglamento surge como un contraste a la norma vigente y por tanto sus modificaciones presentan novedades en diversos aspectos tales como: *"los principios rectores aplicables al tratamiento de datos y condiciones para el consentimiento; la regulación del designado «derecho al olvido» (derecho de supresión de los datos personales); el derecho a la portabilidad de los datos (el interesado tendrá derecho a recibir los datos personales que le incumban); la responsabilidad del responsable del tratamiento (el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento); el registro de las actividades de tratamiento; la notificación de una violación de la seguridad de los datos personales a la autoridad de control; la evaluación de impacto relativa a la protección de datos; la regulación de las transferencias internacionales de datos; y la cooperación entre la autoridad de control principal y las demás autoridades de control interesadas".*

[40] Agencia Española de Protección de Datos: El futuro de la protección de datos. *Asociación Profesional Española de Privacidad. (2020).* Disponible on line: .*https://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/?v=3b0903ff8db1*

4.1 Objeto y ámbito de aplicación del RGPD.

4.1.1. Objeto del RGPD.

Conforme a lo establecido en el art. 1 del Reglamento podemos determinar que el objeto del mismo es la defensa de los derechos y libertades fundamentales de las personas físicas y, en concreto, el derecho a la protección de datos. Por consiguiente, el Reglamento instaura *"las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos."* Por tanto, serán defendidos todos los derechos vulnerados por el trato ilícito de los datos personales.

Del mismo modo, *"la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales."*[41] Este precepto favorece las actividades económicas de los estados miembros y proporcionan una mayor seguridad, respecto a la Directiva, por su carácter imperativo el cual aporta uniformidad legislativa. Ha generado diferentes puntos de vista debido a que podría suscitar conflicto jerárquico entre el valor de defensa de la protección de datos en sí y la libre circulación de estos.

Se determina en el artículo 4 del Reglamento las definiciones de datos personales, tratamiento de datos, fichero y responsable de tratamiento. Estos términos no sufren modificaciones de concepto, pero si se aumenta el numero de términos para una optima interpretación de sus preceptos como el caso de los términos: seudonimización[42], violación de la seguridad de los datos personales[43], tratamiento transfronterizo, normas corporativas vinculantes[44] entre otros.

---

[41] Reglamento (UE) 2016/679. Art. 1.3.

[42] Reglamento (UE) 2016/679. Cit., Art. 4.5.: «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

[43] Reglamento (UE) 2016/679. Cit., Art. 4.12.: «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

[44] Reglamento (UE) 2016/679. Cit., Art. 4.20.: «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

4.1.2. Ámbito de aplicación material y territorial.

Referente al ámbito de aplicación material, el art. 2 del Reglamento dicta que *"El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero."*, es decir, para que pueda darse la aplicación del reglamento el tratamiento de datos ha de estar adjuntos en un fichero[45] de lo contrario no se podría aplicar el RGPD.

El Reglamento en su art. 2, sufre una serie de exclusiones en su ámbito de aplicación material como sería: *"a) el ejercicio de una actividad no comprendida en el ámbito de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de funcionamiento de la Unión Europea (TUE); c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."* Referente la ultima exclusión se someterá a la Directiva (UE) 2016/680[46].

Referente a la aplicación de tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la unión según dicta este mismo artículo será de aplicación el Reglamento (CE) n.o 45/2001[47] adaptándose a las normas del art. 98 del RGPD. Partimos de la base de que la protección que establece el Reglamento se ha de aplicar a las personas físicas indistintamente de su nacionalidad o de su lugar de residencia, en correlación con el tratamiento de sus datos personales.

[45] Reglamento (UE) 2016/679. Cit., Art. 4.6.: «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

[46] Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Diario Oficial nº L 119/89.

[47] Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Diario Oficial nº L 2001-80052.

El RGPD no aborda el tratamiento de datos de las personas jurídicas. Del mismo modo en su considerando 14 abstraemos la idea de no aplicación a datos de empresas constituidas como personas jurídicas. A su vez, según lo establecido en su considerando 27, no se aplicará a la protección de datos de personas fallecidas siendo competencia de los EM la formalización de la normativa del tratamiento de estas.

Para entender el precepto del art. 3, sobre ámbito territorial, se ha de hacer referencia a los conceptos de responsable y encargado. Se entiende por responsable *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"*[48]. En cambio, la figura del encargado está estrechamente vinculada a la del responsable, ya que gestiona el tratamiento de los datos a favor del responsable. Por tanto, el responsable es la autoridad que decide el uso de los datos mientras que el encargado es aquel que lleva a cabo los dictámenes de este.

En el Reglamento observamos que, en lo que atañe a la aplicación territorial ha supuesto, respecto a normativas posteriores, una modificación atrayente ya que la protección del tratamiento de datos se aplica a las actividades de un establecimiento del responsable o encargado en la Unión, indiferentemente de que el tratamiento se haga dentro de la Unión o no.

Del mismo modo, se garantiza la protección de datos de interesados que residan en la UE cuando se realice actividades de tratamiento como la oferta de bienes y servicios independientemente de si se requiere su pago o no, o el control de su actuación independientemente de que el responsable o encargado no es esté establecido en la Unión. Mismamente, se confiere la aplicación de este Reglamento *"al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público."* Este último precepto del art. 3 alude al Derecho Internacional Público y determina la aplicación del RGPD a todo responsable del tratamiento no establecido en la Unión en situación de misión diplomática u oficina consular de un Estado miembro.

[48] RGPD, Art. 4.7.

De forma conclusiva, el Reglamento supone una trasformación en el ámbito de aplicación ofreciendo una protección más amplia establecida para la defensa del tratamiento de datos personales de las personas físicas al margen de su nacionalidad o zona de residencia.

4.2 Competencia judicial internacional.

Las acciones que se remiten frente a encargados o responsables se han de dirigir sobre tribunales competentes del Estado miembro donde estos disponen de un establecimiento como así dicta el artículo 82.6 del RGPD[49] el cual nos dirige al artículo 79.2 de este mism reglamento. Sucesivamente, confiere la elección al reclamante a ejercitar las acciones ante tribunales competentes del Estado miembro donde tenga su residencia.

Las acciones a las que son aplicables el artículo 82 del RGDP tienen naturaleza civil-mercantil y concuerda con el ámbito de aplicación del Reglamento (UE) 1215/2012, conocido como Bruselas I Bis".

En los supuestos de responsabilidad extracontractual se presume la adecuación de la acción en relación con la presencia de un perjuicio conexo con el tratamiento ilícito de datos personales, sin embargo, también cabe la posibilidad de que el tratamiento ilícito de datos provenga de una situación contractual. Conforme a lo establecido por la Jurisprudencia del TJUE toda acción de responsabilidad civil de carácter extracontractual ha de concebirse comprendida en materia contractual en virtud al art. 7 del Reglamento (UE) 1215/2012 "Bruselas I Bis" en caso de que la conducta reprochada conllevase a una violación de las obligaciones contractuales estudiándose el objeto del contrato uno a uno ya que mediante el contrato se puede pactar la responsabilidad del cuidado del tratamiento de datos personales.[50]

Sintetizando encarecidamente en la jurisdicción del establecimiento del responsable, se admite la demanda en el Estado miembro donde el responsable tenga un establecimiento según el art. 79.2 del RGPD. Según lo pronunciado en la STJUE Weltimmo el concepto de establecimiento ha de ser flexible y entenderse como *"cualquier actividad real y efectiva, aun mínima, ejercida*

[49] Reglamento (UE) 2016/679. Cit., art. 82.6.: *"Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2."*
[50] STJUE de 13 de marzo de 2014, Brogsitter, C-548/12.

mediante una instalación estable"[51]. Anexo a ello, debe de apreciarse además el "*grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades la naturaleza especifica de las actividades económicas y de las prestaciones de servicios en cuestión".*

Así mismo, en la STJUE Amazon EU Sàri se contempla la posibilidad de considerar la presencia de un establecimiento en un Estado miembro si no se consta ni de una filial o sucursal, concurriendo la necesidad de evaluar el grado de estabilidad de la instalación y la efectividad del progreso de las actividades en el Estado, concurriendo la posibilidad de plantearse como "establecimiento" un representante de la sociedad si opera con un nivel de estabilidad apto.

Respecto a lo citado, se deduce que todo establecimiento del encargado o del responsable consiente otorgar la competencia a los tribunales del Estado miembro en el cual este situado. Así mismo, la alternativa prevista en el Reglamento reconoce al demandante reclamar en los tribunales donde tenga su domicilio siempre y cuando el demandante tenga un nivel de permanencia que pueda garantizar su estado de estabilidad.

La residencia habitual se puede encontrar en distintos Estados siempre y cuando se halle una relación estricta a ese diferente Estado como puede resultar en el ejercicio de una actividad profesional, además de como la establece la STJUE eDateAdvertising[52] como concepto equivalente al de "centro de intereses de la víctima". Esta forma que determina la competencia del tribunal que ha de tratar la pretensión no resulta la más adecuada debido a la falta de exigencia en el vínculo del centro de intereses y el territorio donde se hace efectivo el daño.

A lo que atañe a esta situación y para ponerla en contexto recurrimos al siguiente ejemplo: Una persona física popular en Alemania y que vive en Francia de forma socialmente anónima es objeto de una calumnia en Francia empleando la lengua alemana. El ciudadano alemán tendrá la opción de demandar ante los tribunales franceses aún no habiéndose producido efectivamente el daño. Por otro lado, si el centro de intereses del ciudadano alemán se hallase en el Estado con el que tiene vínculos profesionales, y no en el Estado de residencia, y el ciudadano alemán hace de forma asidua trabajos de colaboración como tertuliano en un canal televisivo francés en el cual ve afectada su persona ante una serie de calumnias vulnerando así sus derechos a la

[51] STJUE de 1 de octubre de 2015, Weltimmo, C 230/14.
[52] STJUE de 25 de octubre de 2011, eDate Advertising C-509/09 y C-161/10.

personalidad, pero estas calumnias están divulgadas en alemán, no tendría efecto real en Francia.

Por otra parte, la existencia de afinidad de los foros del Reglamento Bruselas I bis y del art. 79.2 del RGDP es debido al hecho de no prejuzgar que se aplique disposiciones implícitas en instrumentos específicos como se indica en el considerando 147 del RGDP[53]. Del mismo modo, especifica en su considerando 145 que *"por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos."*

Según lo trasladado en los párrafos anteriores, podemos afirmar que los foros de competencia del art. 79.2 instaurados en el Reglamento General de Protección de Datos son complementarios a los acopiados por el Reglamento Bruselas I bis. Por consiguiente, la designación de competencia judicial se puede dar según lo dispuesto en el Reglamento Bruselas I bis mediante:

1. En su art. 25 Bruselas I bis. Sumisión expresa. Es considerada una continuación de la autodeterminación de la voluntad al ámbito de la competencia judicial internacional[54]. Conforme lo estipulado en el art. 25, las partes pactan supeditar el litigio ante tribunales competentes de un EM concreto para el conflicto existente o los que puedan surgir debido a la relación jurídica entre las partes siendo esta una medida uniforme resolutoria. Estos acuerdos han de celebrarse por escrito, o verbalmente con posterior certificación escrita o ajustándose a las costumbres determinadas entre las partes.

El escenario descrito se identifica con el artículo 19 del Reglamento Bruselas I bis concerniente a las cláusulas en contratos de consumo[55]. En consecuencia, concebimos que los

[53] Reglamento (UE) 2016/679. Considerando nº147.: En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.o 1215/2012 del Parlamento Europeo y del Consejo deben entenderse sin perjuicio de la aplicación de dichas normas específicas.
[54] Ortega Gimenez, A. (2013). "Imagen y circulación internacional de datos." *Revista Boliviana De Derecho.* Santa Cruz de la Sierra. n. 15, pp. 130-147.
[55] Reglamento (UE) No 1215/2012. Art. 19.3.: "que, habiéndose celebrado entre un consumidor y su contratante, ambos domiciliados o con residencia habitual en el mismo Estado miembro en el momento de la celebración del contrato, atribuyan competencia a los órganos jurisdiccionales de dicho Estado miembro, a no ser que la ley de este prohíba tales acuerdos."

pactos jurisdiccionales pueden perpetuarse en la medida en que se respeten las exigencias de mutuos reglamentos: 1) el requerimiento de compromiso escrito (art. 25 de Bruselas I bis), y 2) la no eliminación de foros que provee el art. 79.2 del Reglamento General de Protección de Datos. En definitiva, los acuerdos han de extender más aun los foros favorables para el afectado.

2. Art. 26 Bruselas I bis. Sumisión tácita. Se entiende que existe sumisión tácita cuando el demandante interpone una demanda ante el tribunal de un EM y el demandado no impugne su competencia judicial iniciando así una discusión sobre el fondo del asunto. El demandado puede declinar la competencia recurriendo a una declinatoria siempre que concurra un pacto de sumisión expreso con anterioridad al pleito o por razón de la materia.

3. Art. 4 Reglamento Bruselas I bis. Foro del domicilio del demandado. La aplicación de este foro para determinar la competencia judicial es uno de los más relevantes de conformidad con el principio actor sequitur forum rei[56]. Dada la circunstancia de una inexistencia de acuerdo expreso o tácito, se establece el foro que atribuye la competencia de los tribunales donde tenga el domicilio el demandado. Para ello, el art. 63 del Reglamento Bruselas I bis concreta la definición de domicilio siendo el domicilio de una persona jurídica el lugar donde se encuentre: *"a) su sede estatutaria; b) su administración central, o c) su centro de actividad principal"*. Por otro lado, tenemos que remitirnos al art. 62 para hallar lo relativo a la residencia habitual de la persona física donde remite a la ley interna del propio Estado. Por ultimo, destacar su escaso uso en la práctica por las distintas desventajas que genera al demandante en cuestiones como idiomas, costes, etc.

4. Ar. 7.3 Reglamento Bruselas I bis. Foro especial en materia de obligaciones extracontractuales. La competencia judicial aplicable mediante este foro lo determina el territorio donde se produce o pueda producirse el daño. Se basa en el principio de ubicuidad haciendo posible al demandante ejecutar una acción por daño eligiendo entre el tribunal del estado donde se efectuó el daño lesivo, siendo este donde se haya producido o donde se padezca el daño. La elección de esta vía puede ser no muy acertada debido a: 1. El inconveniente que genera el forum locus delicti commissi (decretar si por país en donde es ocasionado el perjuicio se ha de entender por el territorio donde se localiza el hecho causal) 2. O el del territorio en que se comprueba el efecto perjudicial.

[56] Principio que establece que el actor debe seguir el fuero del demandado.

Lo indicado en estos últimos párrafos, suponen una clara visión de la fragmentación de la competencia judicial que acomete contra el amparo del individuo del derecho de protección de datos. Pues bien, la STJUE eDate Advertising aparece para disminuir esta fragmentación competencial facultando al perjudicado para que invoque el perjuicio en un EM reclamando un resarcimiento por el menoscabo sufrido ante los tribunales del estado causante de la acción y el Estado donde el perjudicado posee su centro de intereses.

Conforme lo estipulado en el art. 7.2 de Bruselas I bis y en el 79.2 del RGPD podemos observar que su convivencia en el mismo tiempo está en cuestionamiento. Esto es debido a que la jurisdicción ordinaria del Reglamento Bruselas I bis es considerada imparcial, en cambio, la jurisdicción especifica ha revelado que hay un cierto tipo de enlace significativo entre el foro y el asunto jurídico a resolver[57]. Esta afirmación la encontramos en el art. 79.2 del RGPD en sus foros especiales en los que consiente reclamar *"ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento, o ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual"*[58] en situaciones de tratamiento ilícito de datos personales que se desprenden de una responsabilidad extracontractual.

Una vez analizadas estas disposiciones, observamos que una nueva regulacion de las normas de competencia judicial internacional al Reglamento Bruselas I bis podría haber otorgado una unificación de competencia evitando la compleja compatibilidad de foros referentes a esta materia que nos trasladada a dos instrumentos normativos. Del mismo modo, evitar la problemática en litispendencia y conexión con el art. 81 del RGPD para encontrar un punto de inflexión en coherencia entre ambos reglamentos.[59]

Ante la compatibilidad con el Reglamento Bruselas I bis, para paliar las controversias que genera la designación de aplicación de los reglamentos dependiendo de como se ejerciten las acciones, hallamos una doctrina dividida. Pedro de Miguel, sustenta una aplicación acumulativa de los reglamentos con base a los considerandos 145 y 158 del RGPD:

[57] Von Hein, J. (November 07-08, 2016). "Social Media and the Protection of Privacy. Lecture." *European Data Science Conference.* Luxembourg. *p.24*
[58] Reglamento (UE) 2016/679. Art. 79.2.
[59] Reglamento (UE) 2016/679. Cit., art. 81.2 *"Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento".*

> *"Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado […]" y "En los casos en que el presente reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) 1215/2012 del Parlamento Europeo y del Consejo[60] deben entenderse sin perjuicio de la aplicación de dichas normas específicas." [61]*

Del mismo modo, sugiere una revisión y lectura minuciosa de foros del reglamento Bruselas I bis con el fin de no quitar el efecto útil del art. 79.2 del RGPD, como en el caso de sumisión expresa.

La postura contraria la encontramos en Marta Requejo, su argumento se basa en la literalidad del art. 79 del RGPD, el cual instaura un rango imperativo de las normas de competencia que recogen *"las acciones […] deberán ejercitarse"* y en que el amparo del interesado no ha de calificarse como un valor imperioso, *"sino que debe respetar el equilibrio con otros derechos fundamentales, como el de la tutela judicial efectiva, que podría verse afectado si se admite una excesiva proliferación de foros."* También hace referencia al derecho que se solapa en el reglamento con el derecho de protección de datos y es la libre circulación de datos personales como una exigencia para el buen funcionamiento del mercado interior. En caso de percibirse el sistema como gravoso por los responsables o encargados de tratamiento imposibilitando inclusive la permanencia en el mercado se podría estar incurriendo a la falta de protección del derecho de libre circulación de datos.[62]

[60] Reglamento (UE) 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Diario Oficial nº L 351/1.
[61] Asensio, P. A. (2017). Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea. *Revista Española De Derecho Internacional, 69*(1), 75-108. doi:10.17103/redi.69.1.2017.1.03
[62] Requejo Isidro, M. (2017). "La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679." *La Ley Mercantil.* n.42. p.1.

Actualmente no se ha hecho efectiva ninguna decisión del TJUE para resolver la controversia, por tanto, resulta mas consistentes los argumentos que benefician la interpretación restrictiva que impide la aplicación conjunta de ambos reglamentos. Los foros establecidos del RGPD tienen el objeto de adecuarse a una circunstancia determinada, mientras que los foros del Reglamento Bruselas I bis están establecidos para ser aplicados a supuestos generales. Por consiguiente, los principios que son la base de uno y otro reglamento son distintos y excluyentes entre sí, y ha de aplicar la justicia de uno sobre el otro[63], por tanto, el art. 79.2 del RGPD predomina sobre el art. 7.2 del Reglamento Bruselas I bis[64].

Por último, el perjuicio se puede localizar en una relación contractual y por ende supeditarlos a foros concretos del Reglamento Bruselas I bis que operan con un doble cometido: instaurar un foro de amparo especial para el individuo que ha padecido el daño o en situaciones donde los responsables de tratamiento intenten cometer una acción contra los individuos perjudicados, remediar el abandono de foros especiales. Situaciones que constatan lo anterior, serían las relaciones contractuales entre consumidores, un claro ejemplo sería servicios como Facebook o empresas análogas donde se firma un contrato de adhesión encaminado esencialmente a consumidores.

Como ejemplo de lo expuesto encontramos la reciente STJUE Schrems II[65] que solventa el problema de competencia judicial internacional entre Maximiliam Schrems y Facebook Ireland en la que se resuelve la parte civil del caso original del que se ha hecho referencia en el apartado 3. En ella, Schrems apeló acciones judiciales hacia Facebook en Viena usando el foro para consumidores del Reglamento (UE) 44/2001 sin embrago Facebook alegó una excepción de competencia internacional aclarando que el demandante hacia uso de la cuenta como profesional dejando de responder así como consumidor.

La STJUE concluye haciendo referencia a que estos tipos de contratos en lo que atañe a redes sociales puede sufrir variaciones de uso a lo largo de la vida del contrato vigente, por tanto, este contrato se le ha de determina como "dinámico" para adecuar el contrato al objeto y uso que el

[63] Revolidis, I. (2017). Judicial Jurisdiction over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"? *Masaryk University Journal of Law and Technology, 11*(1), 7. doi:10.5817/mujlt2017-1-2
[64] Carrascosa González, J., y Calvo Caravaca, A-L. (2017) *Derecho internacional privado*, Vol. II Comares, Granada, 17ª ed., 2017, pp. 1528.
[65] STJUE de 23 de enero de 2018, Schrems vs. Facebook, C-498/16.

consumidor hace de él. Por último, de la sentencia es destacable también, que la compatibilidad del uso de una red social en actividades tanto comerciales como privadas no supone la no aplicación de amparo hacia los consumidores, por ende, se pueden ejercitar los foros de protección de las normas referentes a la competencia judicial a favor de los consumidores[66].

4.3. Códigos de conducta y certificación.

Entre los aspectos que reglamenta el RGPD hallamos los códigos de conducta y certificación regulados en los arts. 40 a 44. Este instrumento no supone un hecho innovador debido a su previa regulación en la antigua LOPD[67] como códigos tipo, pero sí sufre una trasformación que resulta más interesante.

La posterior LOPD no exigía que fuesen minuciosamente detallados, pero sí tenía que recopilar todos los supuestos de tratamiento y esto ocasionaba un elevado coste de elaboración y mantenimiento por parte de las organizaciones sectoriales. Sin embargo, el RGPD confiere una gran flexibilidad en el momento de crear códigos de conducta.

Según el adjunto a la Dirección de la Agencia Española de Protección de Datos, D. Jesús Rubí Navarrete, hay una importante diferencia respecto a los códigos tipo: *"Los códigos tipo, con el fin de que tuvieran un elevado valor añadido, se exigía que incorporasen el conjunto de actividades de tratamiento de un determinado sector de la A a la Z. El reglamento europeo y la ley de protección de datos dejan bien claro que hay una enorme flexibilidad y que se puede hacer un código de conducta limitado a ciertas actividades sectoriales o limitado a la garantía del ejercicio de ciertos derechos, limitado, en fin, a lo que se quiera."*[68]

[66] Decisión nº 2010/87/UE de la Comisión, 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. Diario Oficial nº L 39 de 12.2.2010, p. 5/18.
[67] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE-A-1999-23750.
[68] Sercon, E. (2019). Los códigos de conducta: una poderosa herramienta de cumplimiento del RGPD - Blog PSN Sercon. Disponible on line: https://blog.psnsercon.com/los-codigos-de-conducta-una-poderosa-herramienta-de-cumplimiento-del-rgpd/

Los códigos de conducta son aplicables en heterogéneos sectores en los que se hayan implantado y serán de imperativo cumplimiento una vez incorporados a ellos tanto por el responsable de tratamiento como por las empresas u organismos.

La adhesión a un código de conducta no es obligatoria, pero estar vinculado a ello, a parte de certificar un excelente grado de cumplimento fomentará un perfil corporativo de garantía. Este compromiso voluntario va en concordancia con la intencionalidad del RGPD de generar una filosofía de cumplimiento de protección de datos y así se ve reflejado en su considerando 98.[69]

Su naturaleza voluntaria tiene una excepción, que es la obligatoriedad que implica la aplicación de estos códigos para las autoridades nacionales, la Comisión Europea y para el Comité europeo de Protección de Datos.

Cabe destacar que, en el RGPD, los códigos de conducta tienen distintos ámbitos de aplicación: Encontramos el subjetivo, que le corresponde determinar a quiénes afecta estos códigos; por otro lado, el ámbito de aplicación objetivo el cual determina la finalidad de su implantación; y, por último, el ámbito territorial que determina los tipos de códigos que se regulan.

1. Ámbito Subjetivo: Los códigos de conducta tienen la potestad de aplicarlos los organismos que estén representando grados de responsabilidad o los encargados de su tratamiento. Del mismo modo, se le confiere la potestad de modificación. En el art. 40.2 se declaran las materias que ampara:

> *"a) el tratamiento leal y transparente; b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos; c) la recogida de datos personales; d) la seudonimización de datos personales; e) la información proporcionada al público y a los interesados; f) el ejercicio de los derechos de los interesados; g) la información proporcionada a los niños y la protección de estos, así*

[69] RGPD. Considerando nº 98.: *"Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento."*

como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño; h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32; i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados; j) la transferencia de datos personales a terceros países u organizaciones internacionales, o k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79."

Por otro lado, se procederá a la aplicación de los códigos de conducta de aquellos que a pesar de no tener el compromiso siendo responsables o encargados, lo realice por el hecho de equipar de garantías imprescindibles en la trasferencia de datos personales a las entidades internaciones o a terceros países. En esto supuesto se ha de establecer mecanismos que resulten jurídicamente vinculantes para convertirse en exigible y vinculante para un tercero.

2. Ámbito objetivo. El objeto de los códigos de conducta es impulsar el cumplimiento normativo entre los organismos de un concreto sector. Para hacer cumplir la normativa en materia de tratamiento de datos personales las empresas han de instaurar normas comunes. Su efectiva adhesión y sometimientos revela una garantía de responsabilidad y respeto normativo.

3. Ámbito territorial. Estos códigos de conducta pueden ser de aplicación nacional y será la autoridad competente quien valorará si tanto el código como sus modificaciones y ampliaciones son conforme a los principios del Reglamento. En caso de que cumpla con las garantías y su compromiso es exigible y avala los derechos de terceros, se registrará y se terminará concluyendo con su publicidad. Por otro lado, otro tipo de código de conducta son los que regulan los tratamientos de datos que se establezcan en más de un EM. En estos supuestos, la autoridad competente remitirá el código al Comité Europeo de Protección de datos para que este resuelva si se ajusta y proporciona las garantías optimas para la trasferencia de datos.

En referencia a la regulación de su supervisión, el art. 41 establece que se asignará tal función a un organismo debidamente acreditado una vez superados los requisitos que establece la autoridad de control competente. Los organismos han de adoptar las medidas necesarias en

supuesto de infracción del código bien por el responsable o por el encargado del tratamiento de datos. Por otro lado, la LOPDGDD promueve la inclusión de mecanismos de resolución extrajudicial de conflictos. Conforme a lo establecido en el art. 83.4.a del RGPD, el incumplimiento del código de conducta supondría una cesación o exclusión del código, del mismo modo, su incumplimiento está vinculado a una sanción administrativa de hasta 10 millones de euros o el 2% de sus ingresos anuales.

Cabe destacar también los códigos de certificación, un concepto nuevo que abarca el RGPD regulados en sus arts. 42 y 43 establecidos como un instrumento voluntario del mismo modo que los códigos de conducta. Se ha de mencionar su previa presencia en la LOPD como un mero mecanismo de supervisión. Su objeto es poner de manifiesto el correcto cumplimiento del RGPD por parte de los responsables y de los encargados de tratamiento.

En su artículo 42.7 establece que *"La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes."* De análoga manera se retirará dicha certificación en los casos de incumplimiento de los requisitos de la certificación por parte de los organismos de certificación que se refiere el art. 43 o por parte de la autoridad de control competente.

En virtud del RGPD, la autoridad de control competente Sin perjuicio de otras funciones en virtud del presente Reglamento, concernirá a cada autoridad de desempeñará las siguientes funciones (art. 57):

> *"a) controlar la aplicación del presente Reglamento; b) promover la comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento; c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento; d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento; e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros; f)*

tratar las reclamaciones e investigarlas; g) cooperar; h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento; [..] m) alentar la elaboración de códigos de conducta y dictaminar y aprobar los códigos de conducta que den suficientes garantías; n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos y aprobar los criterios de certificación de conformidad; o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas; p) elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta y de organismos de certificación; q) efectuar la acreditación de organismos de supervisión de los códigos de conducta y de organismos de certificación. [...]"

Por último, según la LOPDGDD, la aprobación de los códigos de conducta y de certificación lo efectúa la Agencia Española de Protección de Datos o la autoridad autónoma de protección de datos correspondiente cuando dicho código certifique las garantías suficientes. En los supuestos donde los códigos inciden a tratamientos en distintos EM la autoridad de protección de datos antes de su aprobación debe enviarlo al Comité Europeo de Protección de datos y este analizar su conformidad al RGPD y certificar las adecuadas garantías para su trasmisión internacional de datos.

Esta regulación, por tanto, ha supuesto un refuerzo de seguridad del Reglamento sirviendo como garante de cumplimiento de las normas de tratamiento de datos debido a su previa intencionalidad de ajustarse a las normas establecidas. Este instrumento incluso se tiene en cuenta a la hora de imponer sanciones.

4.4. Aspectos positivos y negativos de su implantación.

La implantación del nuevo RGPD ha abordado una situación de inestabilidad en la seguridad de derechos intrínsecos de los ciudadanos de la comunidad europea. Como se ha observado, se ha realizado una modificación de ampliación en el ámbito de aplicación territorial cuyo criterio reside en la residencia del titular de los datos personales independientemente de si el encargado de tratamiento tiene sede o no en la UE. En cambio, la protección que otorgaba la precedente normativa se apoyaba en el establecimiento de la empresa que tratase los datos personales originando así que si una empresa no estaba establecida en un país de un EM de la UE no les era exigibles las garantías determinadas en la normativa.

Otro aspecto destacable es la implantación positiva de distintos aspectos de protección como es el caso de la realización de una categórica prevención en el tratamiento de datos y en caso de violación de seguridad la trasmisión de una obligada notificación. Paralelamente, la declaración de consentimiento también ha sido implantada para mejorar y evitar que el mero silencio o la inacción pudiese dar la potestad a la empresa del libre tratamiento de datos. En este aspecto encontramos inclusive la opción de prestar el consentimiento granular, es decir, autorizar el tratamiento de datos personales con diversas finalidades.

Una de las medidas más atrayentes son las sanciones que se establecen a las empresas con el objeto de conseguir un compromiso real de cumplimiento de la norma a la hora de efectuar el derecho a la portabilidad de los datos y la libertar otorgada a las empresas para que determinen y elijan las medidas de seguridad mas idóneas para proteger los datos personales. Se ha de considerar el RGPD como un instrumento generador de consciencia sobre el valor de los datos y un impulsor a la seguridad proactiva.

Sin embargo, algunos expertos en materia de protección de datos encuentran una serie de vicisitudes que pueden hacer notoria la necesidad de una modificación en algunos preceptos:

Samuel Sarra nos afirma la existencia de un gran numero de disposiciones donde encontramos ambigüedades en expresiones tales como “medidas razonables”, “sin dilaciones”, “no más tiempo del necesario”, “cuando sea técnicamente posible”, etc. Esto es el resultado de una inseguridad jurídica donde el destinatario de la norma entraría en una tesitura de desconcierto a la hora de hacer cumplir la normativa. El ejemplo que muestra en referencia al tratamiento de menores de edad es el siguiente: *“¿cómo debe el responsable del tratamiento asegurarse que el consentimiento fue dado por sus padres? El RGPD dice que mediante "esfuerzos razonables", pero, ¿qué es un esfuerzo razonable?”.*[70] La pregunta lanzada, entre otras, cuestiona la seguridad jurídica la cual ha sido el objeto de esta nueva normativa, por tanto, a pesar de solucionar ciertas problemáticas de la anterior normativa sigue existiendo pequeñas pinceladas que denota una normativa que lucha por palpar la excelencia, pero sigue sin conseguirla.

[70] Lo mejor y lo peor de la nueva normativa de privacidad, según los expertos. *ABC.* (2018). Disponible on line: https://www.abc.es/tecnologia/redes/abci-rgpd-mejor-y-peor-nueva-normativa-privacidad-segun-expertos%20201805242219_noticia.html?ref=https:%2F%2Fwww.google.com%2F

En la misma línea, explica Jesús Yáñez la carencia de concreción del RGPD: *"nos encontramos con un Reglamento muy poco concreto en el que pasamos de unas obligaciones totalmente tasadas en nuestra LOPD a una normativa en la que existen grandes inseguridades jurídicas como los conceptos de tratamiento a gran escala para, por ejemplo, saber si tenemos que designar un delegado de protección de datos. El Reglamento Europeo exige que las entidades sean conscientes de sus riesgos y actúen en consecuencia, pero muchas veces sin decir cómo, lo que supone una libertad de actuación que, en muchas ocasiones, genera cierto desasosiego sobre si están haciendo bien las cosas".*[71]

Por otra parte, encontramos una crítica al principio de consentimiento, en este caso Borja Adsuara, experto en Derecho, Estrategia y Comunicación Digital, nos hace referencia a una degradación de este principio poniéndolo *"al mismo nivel de lo que eran y deberían seguir siendo unas excepciones, muy fundamentadas: el "interés público" o el "interés legítimo" de una empresa por tratar nuestros datos personales sin nuestro consentimiento"* Con esta afirmación, crea la percepción de la posibilidad de "una puerta de atrás" a la hora de pedir el consentimiento de los titulares de datos.

Otros de los efectos negativos que ha supuesto la implantación del RGPD a las que alude otros especialistas como Pablo Fernández Burgueño, abogado especializado en blockchain, ciberseguridad y marketing online, son las nuevas cargas que han surgido para el cumplimiento de este. Pese al trascurso de tiempo acontecido hasta su imposición hubo empresas que tardaron mas de lo esperado en la implementación de medidas internas necesarias para adaptarse a la normativa. En muchos casos debido a una alarmante dejadez por parte de la Agencia Española de Protección de Datos "*de la que he llegado a recibir respuestas telefónicas indicando que el reglamento no había entrado en vigor o que aún tenía que ser objeto de transposición. La desinformación y la desidia por parte de la autoridad de control han conducido a que un número importante de empresas españolas no hayan podido abordar adecuadamente sus adecuaciones o lo hayan hecho de forma precipitada y con errores graves que los ha llevado*

[71] O, A. (31 de mayo de 2018) "Implantación del RGPD: problemas y soluciones". *Expansión.* Disponible on line: https://www.expansion.com/juridico/actualidad-tendencias/2018/05/31/5b101f93e5fdeaa94e8b4578.html

a, por ejemplo, pedir innecesarias renovaciones de consentimientos para el envío de comunicaciones publicitarias por vía electrónica."[72]

[72] Lo mejor y lo peor de la nueva normativa de privacidad, según los expertos. *ABC.* (2018). Disponible on line: https://www.abc.es/tecnologia/redes/abci-rgpd-mejor-y-peor-nueva-normativa-privacidad-segun-expertos%20201805242219_noticia.html?ref=https:%2F%2Fwww.google.com%2F

5. CONCLUSIONES.

El estudio demuestra que en un contexto globalizado la intencionalidad de dotar un sistema legislativo con normativas nacionales o regionales resulta ineficiente y limitado. Por ello, las instituciones de la UE han sido transcendentales en la búsqueda de una legislación versátil y próspera para solventar las controversias planteadas en materia de protección de datos. La creación de un eminente sistema de protección de datos como fue la Directiva 95/46/CE supuso un positivo cambio en este ámbito, sin embargo, fue improbable predecir el progreso del entorno digital y su futura decadencia debido a su normativa desfasada que obligó la reestructuración normativa.

Para ello, el transcurso de una serie de controversias manifestadas ante la justicia europea como la STJUE de nulidad de la Decisión 2004/535/CE, la STJUE Google Spain y la STJUE Schrems marcaron un antes y un después en la normativa europea. El caso Schrems declaró la derogación de la Directiva 95/46/CE fundamentándose en la vulneración del derecho de protección a la vida privada y de la tutela efectiva (debido a no existir en el derecho interno de los EEUU recursos eficaces para que los ciudadanos europeos pudiesen alegar una vulneración en sus derechos) junto con la ilegitimidad para fundar sus acciones con el argumento de seguridad nacional puesto que no constataba en la normativa interna de EEUU el tratamiento de datos destinadas a limitar las posibles injerencias en derechos fundamentales.

Por consiguiente, se implantó el Reglamento 2016/679 para corregir los fallos de contenido de las anteriores legislaciones. Se pasó de un modelo reactivo a uno proactivo, de un acto legislativo no vinculante a uno vinculante, en definitiva, se estableció una unificación y una integridad legislativa que concernía a todos los Estados Miembros. Incorporaciones tales como el derecho al olvido, la obtención del consentimiento para el tratamiento de datos personales, el derecho de rectificación, oposición, cancelación, la introducción de códigos de conducta y certificación y su mejora en el ámbito de aplicación territorial han supuesto un contenido más modernizado y uniforme, por tanto, se considera incuestionable el gran avance aportado respecto a protección de datos. Sin embargo, el estudio pretende contextualizar el derecho de protección de datos y dar una visión del presente y futuro de la actual normativa. Por ello, destacamos el hecho de que esta normativa no estará exenta de modificaciones debido a las existentes deficiencias en la normativa, como bien se analiza en el trabajo, por tanto, tendrá que

someterse a una permuta constante para adecuarse a una comunidad que no termina de avanzar y progresar.

En lo que respecta al ámbito de aplicación territorial, destacamos la extensión de la legislación generando una notoria mejora puesto que además de a responsables o encargados de tratamiento con establecimiento en la Unión, es de aplicación a aquellos de terceros países que traten datos de ciudadanos de la UE, ya sea de cara a la oferta de bienes o servicios, o para el control de su comportamiento (en cierta medida en que este tenga lugar en la UE), aunque no esté establecido físicamente en el territorio de la UE. Para la efectividad de esta extensión del ámbito de aplicación, las organizaciones tendrán que designar un representante en la Unión Europea, que funcionará contacto directo con las Autoridades de supervisión y con los ciudadanos. Esta modificación supone para las empresas, que antes no estaban obligadas por la legislación de protección de datos de la UE, convertirse inmediatamente en responsables del tratamiento de datos personales, por tanto, han de llevar a cabo el cumplimiento de las disposiciones que se establecen en el Reglamento.

Por otra parte, la cuestión de competencia internacional judicial determina qué pleitos internacionales pueden ser solventados por unos tribunales o por otros. El vigente sistema de competencia internacional judicial está regulado por una disparidad de legislaciones como convenios internacionales, reglamentos de la UE y normativas internas. De este modo, el Reglamento General de Protección de Datos ha manifestado asumir una misión evidente, brindar al perjudicado la facultad de llevar a cabo el amparo de sus derechos en el EM que desee dando prioridad al Estado del domicilio habitual del perjudicado siempre y cuando el perjudicado pueda asegurar que su permanencia esté en situación de estabilidad. Los supuestos que se aplican en el art. 79 del RGPD son principalmente controversias de naturaleza civil enfocados a una petición de responsabilidad contractual o extracontractual cuya aplicación de determinación de competencia estaba regulada previamente por reglamento Bruselas I bis. El juego de las reglas de competencia internacional judicial, en referencia a la aplicación de uno u otro reglamento, está aún sin resolver debido a la ausencia de una decisión del TJUE que solvente la problemática. La consonancia relativa de foros con el Reglamento Bruselas I bis en virtud de su entendimiento conjunto con el RGPD consiente disminuir la falta de foros especiales para el responsable, al mismo tiempo que amplía disposiciones de foros para el perjudicado.

No obstante, dispone de más contundencia las alegaciones en defensa de una interpretación estricta, que imposibilita la aplicación mixta de uno y otro reglamento. Por tanto, entendemos que los principios que inspiran ambos reglamentos son diferentes, y por ello, prevalece uno sobre el otro, siendo el artículo 79.2 del RGPD el que se imponte sobre el artículo 7.2 del Reglamento Bruselas I bis. La convivencia de ambas normativas genera una difícil interpretación la cual se considera que hubiera sido más sencillo resolver si se hubiese trasferido la determinación de la competencia judicial directamente al Reglamento Bruselas I bis.

Cabe destacar también, que el Reglamento establece que la Comisión y las autoridades de control, en referencia con organizaciones internacionales y terceros países, realicen la elaboración de instrumentos de cooperación internacional con el objeto de contribuir a la aplicación eficaz de los preceptos legislativos concernientes a la protección de datos. De análoga manera, proporcionarse mutuamente ayuda a nivel internacional en la aplicación de la legislación de protección de datos a través de notificación, intercambio de información y la remisión de reclamaciones. Todo ello, establece las bases para alcanzar las metas de desarrollo en materia de protección de datos.

Otro aspecto a destacar del estudio es la implantación del RGPD de un valioso y eficaz mecanismo de responsabilidad proactiva que facilita la descripción de conductas adecuadas, éticas y legales que sirven como garante de los principios de la protección de datos desarrollados en este reglamento, conocido como los códigos de conductas. Estos suponen una adhesión voluntaria, pero en caso de ser adheridos a un código de conducta este ha de ser vinculante y de exigible cumplimiento. Su aplicación corresponde a organismos que estén representando categorías de responsabilidad o aquellos encargados de su tratamiento. Encontramos dos tipos de códigos: los de ámbito nacional y los que regulan tratamientos de datos que se dan en más de un EM de la UE. Así mismo, se regula también los códigos de certificación que sirve como un mecanismo que acredita el cumplimiento del RGPD por parte de los responsables de tratamiento de datos mediante la utilización de sellos o marcas.

Las novedosas y exitosas cuestiones que han establecido una gran mejora en materia de protección de datos con la entrada en vigor del Reglamento General de Protección de datos se contrarrestan debido a la existencia de algunos defectos de contenido. Las ambigüedades de expresiones que generan inseguridad jurídica, el tratamiento de los datos personales sin consentimiento debido a un interés publico o legítimo, y las cargas que ocasionó el

cumplimiento del RGPD estimula un necesario reforzamiento en el derecho de protección de datos. Por ello, es de vital necesidad seguir adecuando el equilibrio entre el progreso económico y la defensa de un derecho fundamental. Esta culminación irá llegando con la futura jurisprudencia que solucionará los defectos del RGPD surgidos por el continuo avance tecnológico y social, del mismo modo que sucedió con la Directiva 95/46/CE, con el objeto de proteger y garantizar a los titulares de datos un efectivo poder de disposición sobre su propia información.

6. BIBLIOGRAFÍA.

Asensio, P. A. (2017). Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea. *Revista Española De Derecho Internacional*, *69*(1), 75-108. http://dx.doi.org/10.17103/redi.69.1.2017.1.03

Carrascosa González, J., y Calvo Caravaca, A-L. (2017) *Derecho internacional privado*, Vol. II Comares, Granada, 17ª ed., 2017, pp. 1528.

De Miguel Asensio. P. (2017) "Competencia y Derecho aplicable en el Reglamento General sobre protección de datos en la UE." *Revista Española de Derecho Internacional.* Madrid. Vol. 69/1, pp. 75-108. http://dx.doi.org/10.17103/redi.69.1.2017.1.03

Herrán Ortiz, A. I. (2002). *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales*. Dykinson, Madrid, pp. 388.

Ortega Gimenez, A. (2013). "Imagen y circulación internacional de datos." *Revista Boliviana De Derecho.* Santa Cruz de la Sierra. n. 15, pp. 130-147.

Ortega Giménez, A. (2015) "*La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*" *AEPD*, Madrid, p. 23, y *Transferencias internacionales de datos de carácter personal ilícitas*, Cizur Menor, Aranzadi (2017), p. 31.

Puerto, M. I., y Sferrazza Taibi, P. (2017). "La sentencia Schrems del Tribunal de Justicia de la Unión Europea: Un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional." *Revista Derecho Del Estado*, (40), 209-236. http://dx.doi.org/10.18601/01229893.n40.09.

Requejo Isidro, M. (2017). "La aplicación privada del derecho para la protección de las personas físicas en materia de tratamiento de datos personales en el reglamento (UE) 2016/679." *La Ley Mercantil.* n.42. p.1.

Revolidis, I. (2017). Judicial Jurisdiction over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"? *Masaryk University Journal of Law and Technology, 11*(1), 7. http://dx.doi.org/10.5817/mujlt2017-1-2

Von Hein, J. (November 07-08, 2016). "Social Media and the Protection of Privacy. Lecture." *European Data Science Conference.* Luxembourg. *p.24*

7. WEBGRAFÍA.

Agencia Española de Protección de Datos (2020) "El futuro de la protección de datos. *Asociación Profesional Española de Privacidad"* Disponible on line: *https://www.apep.es/aepd-el-futuro-de-la-proteccion-de-datos/?v=3b0903ff8db1*

Parlamento Europeo. "La protección de datos personales." *Fichas temáticas sobre la Unión Europea*. Disponible on line: https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

Lo mejor y lo peor de la nueva normativa de privacidad, según los expertos. *ABC.* (2018). Disponible on line: https://www.abc.es/tecnologia/redes/abci-rgpd-mejor-y-peor-nueva-normativa-privacidad-segun-expertos%20201805242219_noticia.html?ref=https:%2F%2Fwww.google.com%2F

Macaskill, E y Dance, G (2013) "NSA files: Decoded." Disponible on-line: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/2

O, A. (31 de mayo de 2018) "Implantación del RGPD: problemas y soluciones". *Expansión.* Disponible on line: https://www.expansion.com/juridico/actualidad-tendencias/2018/05/31/5b101f93e5fdeaa94e8b4578.html

Quejas contra Facebook Ireland Limited (2011). Disponible on line: http://www.europe-v-facebook.org/ES/Quejas/quejas.html

Schrems, M (2013). "Complaint against Facebook Ireland Ltd – 23 PRISM". Disponible on line: http://www.europe-v-facebook.org/prism/facebook.pdf

Sercon, E. (2019). Los códigos de conducta: una poderosa herramienta de cumplimiento del RGPD - Blog PSN Sercon. Disponible on line: https://blog.psnsercon.com/los-codigos-de-conducta-una-poderosa-herramienta-de-cumplimiento-del-rgpd/

Supervisor Europeo de Protección de Datos. Unión Europea. Disponible on line: https://edps.europa.eu/

Terdiman, D (2013) "Zuckerberg touts Facebook's mobile strength, says US 'blew it' on NSA." *CNET*. Disponible on line: https://www.cnet.com/news/zuckerberg-touts-facebooks-mobile-strength-says-us-blew-it-on-nsa/

U.S Department of the Treasury. "Terrorist Finance Tracking Program (TFTP)". Disponible on line: https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp

ANEXO 1

REFERENCIAS LEGALES O JURISPRUDENCIALES

- Convenio nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos trasfronterizos de datos. BOE-A-1985-23447

- Decisión. nº 2000/520/CE, comisión de las comunidades europeas, de 26 de julio de 2000, 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. Diario Oficial nº L 215/7.

- Decisión nº 2010/87/UE de la Comisión, 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. Diario Oficial nº L 39 de 12.2.2010, p. 5/18.

- Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Diario Oficial nº L 119/89.

- 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. Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050.

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE-A-1999-23750.

- Programa de Estocolmo - Una Europa abierta y segura que sirva y proteja al ciudadano del Consejo Europeo, de 4 de mayo de 2010. Diario Oficial nº C 115 /1.

- Reglamento (CE) nº 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Diario Oficial nº L 2001-80052.

- Reglamento (CE) no 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»). Diario Oficial nº L 199/40.

- Reglamento (UE) 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil. Diario Oficial nº L 351/1.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (Reglamento general de protección de datos). Diario Oficial nº L 119 de 4.5.2016, p. 1/88.

- 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. Diario Oficial nº L 295/39.

- Reglamento del Parlamento Europeo y del Consejo, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Diario Oficial nº L-2016-80807.

- Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea que entró en vigor el 1 de diciembre de 2009. Diario Oficial nº C 306 de 17.12.2007, p. 1/271.

- STJUE de 1 de octubre de 2015, Weltimmo, C 230/14.

- STJUE de 13 de marzo de 2014, Brogsitter, C-548/12.

- STJUE de 17 de mayo de 2004, C-317/04 y C-318/04.

- STJUE de 23 de enero de 2018, Schrems vs. Facebook, C-498/16.

- STJUE de 25 de octubre de 2011, eDate Advertising C-509/09 y C-161/10.