PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

APLICACIÓN EXTRATERRITORIAL DE LA LEY: EL CASO DEL REGLAMENTO DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

TESIS PARA OPTAR AL GRADO ACADÉMICO DE MAGÍSTER EN DERECHO INTERNACIONAL ECONÓMICO

AUTORA

Jackeline Gisela Magallanes Pacherre

ASESOR

Quindimil, Manuel Angel

Lima, 2020

A la mujer que más admiro, mi madre.

Resumen

El presente trabajo analiza las implicancias del Reglamento General de Protección de Datos de la Unión Europea, en relación al carácter extraterritorial, que esta normativa señala.

En el Capítulo I se desarrolla la legislación y la jurisdicción extraterritorial desde la evolución de estos conceptos en el derecho internacional público, sobre la base de la globalización y los avances tecnológicos de las comunicaciones.

En el Capítulo II se hace referencia al concepto de datos personales y el derecho a la protección de los mismos, con mención de las diferencias en su tratamiento por parte de los Estados Unidos de América y por parte de la Unión Europea, enfatizando en el sustento y la lógica disímil entre estos sujetos de derecho internacional y los principios que priorizan y consagran.

En el Capítulo III se analiza la aplicación "extraterritorial" del Reglamento desde el punto de vista jurídico y fáctico, señalándose los principales desafíos que trae consigo esta normativa, la conveniencia y problemática de su implementación para la continuidad del comercio con los ciudadanos europeos y la reputación de las empresas.

Asimismo, se comentan algunas de las principales resoluciones emitidas por las autoridades europeas en materia de protección de datos personales, así como los últimos pronunciamientos del Tribunal de Justicia de la Unión Europea que analizan los alcances del Reglamento General de Protección de Datos.

Finalmente, se hace una breve referencia a la legislación peruana, y el enfoque de la misma en relación con los antecedentes que se describen.

ÍNDICE

CAPÍTULO III

CAPÍTULO IV

INTRODUCCIÓN

La protección de datos personales es un derecho que ha sido desarrollado principalmente en Europa, teniendo su origen en la Convención Europea de Derechos Humanos, adoptada en 1950 y vigente a partir de 1953, que preceptúa, en su artículo 8.°, el derecho al respeto a la vida privada y familiar, siendo el Tribunal Europeo de Derechos Humanos la máxima autoridad jurisdiccional para la garantía de los derechos fundamentales en Europa.

En la fecha en que empezó a redactarse el presente trabajo, se aproximaba la entrada en vigencia del Reglamento de Protección de Datos Personales de la Unión Europea, que reemplaza a la Directiva 95/46/EC. La novedad e implicancias jurídicas que dicho reglamento traía, es la mención del alcance extraterritorial de su propia regulación, lo que en principio se podría interpretar como el alcance de esta normativa terceros países no miembros de la Unión Europea, sin que necesariamente se tenga instalado algún procesador o sede en algún lugar de Europa.

En el contexto de la dinámica propia de las redes y de la evolución de la tecnología, la normativa que adoptan los países u organizaciones internacionales puede diferir entre ellos, o incluso contraponerse, dados los diferentes enfoques con los que se visualiza a los derechos relacionados con la protección de datos personales y la preeminencia que le otorga cada Estado u organización internacional.

La nueva normativa europea sobre protección de datos personales establece su carácter extraterritorial, surgiendo con ello un debate alrededor del concepto clásico de jurisdicción como elemento central del poder de cada Estado, para regular y hacer cumplir lo normado, poder que es consustancial a la idea de una autoridad de gobierno y territorio.

El alcance extraterritorial de la normativa sobre protección de datos personales se contrapone al tradicional concepto de territorialidad, y ha sido desarrollado, previamente, en la

jurisprudencia emitida por el Tribunal de Justicia de la Unión Europea, en adelante TJUE, en numerosos casos.

Uno de los más emblemáticos casos, en materia de protección de datos, es el caso *Google Spain* SL y *Google Inc*. por un lado, y por otro lado la Agencia Española de Protección de Datos y el señor Costeja González —ciudadano español— en relación con la reclamación del Sr. Costeja González contra ambas sociedades sobre el retiro de sus datos de los motores de búsqueda de Google, reclamos que fueron amparados por el Tribunal, mediante sentencia de fecha 13 de mayo de 2014.

En el citado caso, el Sr. Costeja González solicitaba la eliminación de ciertos datos que surgían en la búsqueda en *Google*, empresa que, expuso como defensa, entre otros argumentos, que *Google Inc*. propietaria de *Google Spain SL*, se encontraba constituida en Estados Unidos de América y por tanto se regían por la legislación estadounidense y; que además del análisis de ponderación de derechos, debería resultar la primacía del derecho a la libertad de expresión e información, sobre los derechos alegados por el reclamante.

En la comentada decisión judicial, el TJUE desarrolló a nivel jurisprudencial, el denominado "derecho al olvido" que posteriormente ha sido regulado en el Reglamento de Protección de Datos de la Unión Europea (RGPDUE) que entró en vigor el 25 de mayo del 2018.

Esta nueva reglamentación suponía un alcance extraterritorial como respuesta a la dinámica actual del tráfico por internet en medio del fenómeno de la globalización y la búsqueda de una normativa que dote de efectividad a la protección de datos personales, en especial frente al sistema norteamericano, donde se han originado y residen las principales compañías de productos y servicios informáticos. En dicho contexto, la interrogante surge en virtud de los desafíos jurídicos y económicos que traen consigo las disposiciones contenidas en el RGPDUE.

CAPÍTULO I

De la extraterritorialidad de la ley

La noción de extraterritorialidad y los alcances de la jurisdicción y su evolución, de territorial a universal, son los aspectos que desarrollaremos en el presente capítulo.

En relación con el término "extraterritorialidad", el Reporte de la Comisión de Derecho Internacional de la Organización de las Naciones Unidas, sesiones 15-18 del 1 de mayo, 9 de junio, 3 de julio y 11 de agosto del 2006, señala que:

> La extraterritorialidad tiene lugar cuando un Estado abarca la zona más allá de su territorio, incluidas sus tierras, aguas interiores, mar territorial y espacio aéreo adyacente. El área más allá del territorio de un Estado puede caer dentro del territorio de otro Estado o puede estar fuera de la jurisdicción territorial de cualquier Estado, a saber, alta mar y espacio aéreo adyacente, y espacio ultraterrestre.
>
> Con respecto a la ley aplicable, la noción de jurisdicción extraterritorial puede ser entendida como el ejercicio de la jurisdicción de un Estado con respecto a su legislación nacional, en su propio interés nacional más que la aplicación de la ley extranjera o el derecho internacional. (p. 230)

Un concepto que predomina, y, en ello, los juristas también han coincidido, es que la extraterritorialidad se define como una ficción del derecho internacional que ha sido empleada o utilizada para sustentar las inmunidades que son inherentes a ciertas personas o a ciertas cosas, como si estuviesen en territorio nacional y pertenezcan a otro país o Estado soberano, como es el caso de las embajadas y/o funcionarios diplomáticos. También se señala que, la extraterritorialidad tiene validez jurídica en cuanto a los barcos o buques de guerra que se encuentran en alta mar o puertos extranjeros, entendiéndose que no pueden ejercerse actos

coercitivos a bordo por parte del Estado dominante, así como detener al individuo o persona que haya cometido un acto delictivo en su país, por lo que no podrá ser juzgado allí con las normas que a este le rigen si no por las que le rigen al propio.

En el Diccionario de Ciencias Jurídicas, Políticas y Sociales de Ossorio podemos encontrar la perspectiva y posición del autor con respecto al principio de extraterritorialidad. Así, señala:

> En el Derecho Internacional Público se admite que los agentes diplomáticos de un país acreditados en otro disfruten de determinados privilegios e inmunidades, derivados principalmente de una ficción jurídica, consistente en suponer que siguen residiendo en el territorio que representan y no en el territorio en que ejercen su representación.
>
> […] La extraterritorialidad se extiende a las naves de guerra surtas en puertos extranjeros o que navegan en aguas jurisdiccionales ajenas. Actualmente, la ficción de la extraterritorialidad es muy discutida en la doctrina, justificándose los precitados privilegios por otras consideraciones, tales como las de reciprocidad, la necesidad de que puedan ejercer sus funciones con independencia, etc. Tampoco la doctrina es unánime en la determinación de las personas a quienes alcanza el derecho de extraterritorialidad, lo mismo en lo que afecta al personal de la misión que a los familiares de los agentes diplomáticos. (Ossorio 2014: 399)

En dicho contexto, podemos señalar que, el carácter extraterritorial del Reglamento de Datos de la Unión Europea pretendería su aplicabilidad más allá de sus fronteras, con la finalidad de proteger los derechos que consagra su regulación.

1.1. **De la evolución del Derecho Internacional Público**

En relación con el derecho internacional público comenta el jurista peruano Raúl Chanamé Orbe que, la extraterritorialidad se aplica a determinadas personas como son los agentes

diplomáticos, embajadores o funcionarios de alto nivel enviados en una delegación especial a tratar temas específicos. De esta manera señala el autor que:

> En derecho, se entiende por sistemas de extraterritorialidad aquellos en los que la jurisdicción y leyes de un Estado soberano no se aplican a determinadas personas que se encuentran en su territorio. El principio de extraterritorialidad, más conocido con el nombre de inmunidad, se aplica a las delegaciones diplomáticas, agentes diplomáticos y consulares, y parte de sus bienes, así como a los buques de guerra extranjeros que se hallan en Estado distinto que al de su pabellón, pues se entiende que un buque, se encuentre en el puerto en el que se encuentre o en altamar, forma parte del territorio de la nación de la bandera que enarbola. […]. Es una ficción jurídica que se refiere a la extensión de territorio de un país, este precedente en el caso de las embajadas, que son consideradas como parte del territorio del país extranjero y no del país que naturalmente le debería pertenecer. (Chanamé 2014: 387)

Esta premisa nos permite concluir que, tradicionalmente, el concepto de extraterritorialidad se entendía relacionado al concepto de inmunidad en el contexto de la diplomacia internacional.

Para Koskenniemi (2010) "el Derecho Internacional Público es un conjunto de reglas e instituciones, pero, a su vez, es una tradición y un proyecto político". En ese sentido, el Derecho Internacional Público viene a ser el ordenamiento jurídico que regula la relación y el comportamiento de los Estados y otros entes internacionales, en sus competencias inherentes, propias y en sus relaciones mutuas, acerca del fundamento de incuestionables valores simples, para mantener la paz y la cooperación internacional por medio de normas que emanan de las fuentes internacionales específicas, ampliamente conocidas por la doctrina, como lo son los

tratados internacionales, costumbre internacional, principios generales del Derecho y, de manera auxiliar, la jurisprudencia y la doctrina internacional.

En la actualidad, el derecho internacional, que sistematiza los vínculos pacíficos y de confraternidad entre los Estados, se halla sujeto a un gran desarrollo, en lo que respecta al tema procesal.

En cuanto a los derechos subjetivos en el ámbito internacional, según señala Salmón (2007) "La afirmación de la subjetividad internacional del individuo constituye, sin duda alguna, uno de los signos del Derecho Internacional de nuestros días. Tras la barbarie de la Segunda Guerra Mundial es que la comunidad internacional tomará conciencia de la importancia de hacer valer estos derechos en el orden internacional." (p. 245)

Si bien, por su propia naturaleza se le ha reconocido a los derechos humanos, un ámbito de protección internacional, esta situación no implica la perdida de la soberanía de los Estados, conforme nos comenta Salmón (2005):

> Sin embargo, esto no significa, y creemos que es importante poner el énfasis aquí, que el Estado y su soberanía hayan desaparecido, sino que los derechos humanos y la soberanía han de coexistir y condicionarse recíprocamente. Los derechos humanos, por tanto, han erosionado, pero no destruido el concepto de soberanía. En efecto, un Estado de Derecho tiene como uno de sus fines primordiales la protección de los derechos de las personas, pues estos constituyen la piedra angular de todo ejercicio de la soberanía estatal. (p. 152).

La búsqueda de justicia en temas universales da lugar a su vez al principio de extraterritorialidad, que se ve reflejado tanto en la legislación como en la jurisdicción.

1.2. **De la noción actual de extraterritorialidad**

Para poder ahondar en el tema de investigación, es necesario señalar que el concepto de extraterritorialidad, actualmente, no se restringe al ámbito de la diplomacia, sino que su concepción ha variado en el tiempo, a decir de Parrish (2017):

> Superar el principio de soberanía territorial como una definición del principio del derecho internacional y el intento de cambiar los principios jurisdiccionales tienen un atractivo comprensible a corto plazo. Primero, la territorialidad estricta ha sido descartada por los conceptos de libertad individual y razonabilidad, y también en la doctrina del conflicto de leyes. Segundo, las soluciones transnacionales a menudo se demandan en un mundo integrado y globalizado, dada la facilidad de transporte y comunicación modernos, el crecimiento del comercio y corporaciones multinacionales que hacen negocios a través de las fronteras, desarrollos tecnológicos como internet y el surgimiento de organizaciones delictivas transnacionales. Tercero, como los Estados Unidos tienden a estar menos dispuestos a celebrar tratados y cooperar multilateralmente, la necesidad de encontrar otras soluciones para atemperar los aspectos negativos de la globalización se hizo más apremiante. (p, 219)

Conforme con lo comentado, el principio de extraterritorialidad, ha cobrado mayor relevancia, en el contexto de la globalización, en esta línea, señala Hernández (2010):

> La globalización económica diseña un marco jurídico, político y económico en el que las empresas transnacionales se desenvuelven sin contrapesos suficientes. El Derecho Internacional de los Derechos Humanos no tiene articulados sistemas jurídicos capaces de someter a las multinacionales a control. Tanto los sistemas universales de protección de los derechos humanos y laborales fundamentales, como los códigos externos ad hoc y los internos no pueden neutralizar la fortaleza de la Lex Mercatoria. (p. 272)

En efecto, la dinámica del mercado y el interés en contratar bienes y servicios de manera rápida son el contexto ideal para que puedan darse transferencias de datos que no resguarden adecuadamente los datos personales, situación que preocupa a los legisladores.

Mencionaremos como ejemplo a los Estados Unidos de América, porque este país por mucho tiempo ha gozado de una hegemonía económica que, le ha permitido dictar normativa que suponía para sí misma un alcance extraterritorial.

Al respecto, se comenta en Parrish (2017: 6-7):

> Los años 1990 y 2000 fueron testigos de un aumento dramático en el número de leyes nacionales aplicadas a la conducta extranjera. El crecimiento comenzó en el contexto del derecho privado, con las leyes antitrust y de valores. Las áreas de derecho público siguieron pronto. A fines de la década de 2000, los académicos acogieron con satisfacción el uso de los tribunales nacionales y los conceptos ampliados de jurisdicción universal como método alternativo de promover la responsabilidad y exportación de una marca particular de justicia.

La regulación que pretende un extraterritorial también ha sido imitada por otros países. De esta manera, señala (Parrish 2008):

> Que otros países hayan seguido el ejemplo extraterritorial estadounidense no es sorprendente. Con el tiempo, la amplia aplicación de los Estados Unidos de su propia ley extraterritorialmente ha creado un precedente (si no un sentido de rectitud). De hecho, el uso de leyes extraterritoriales por otros países ha dado lugar a algunos casos muy publicitados. Desde internet, cibercafés, enjuiciamientos criminales y casos prominentes de derechos humanos, así, otros países han comenzado a usar sus leyes como una forma de avanzar en sus propias políticas exteriores y responder a la aspiración estadounidense percibida de especial estatus legal. A medida que Estados Unidos ha intensificado sus reclamos de jurisdicción extraterritorial, otros países

> reclaman “yo también”. En muchos sentidos, el uso de leyes nacionales para abordar los desafíos transnacionales se está convirtiendo en una norma internacional. (pp. 855-856)

En resumen, lo que viene aconteciendo es la emisión de normativa que pretende un alcance extraterritorial con la finalidad de proteger los derechos que consagra el Estado emisor de dicha legislación y de sus ciudadanos más allá de sus fronteras.

1.3 **Jurisdicción extraterritorial**

En el contexto analizado, corresponde comentar sobre la jurisdicción, definida en palabras de Chiovenda (1954), como:

> La función del Estado que tiene por fin la actuación de la voluntad concreta de la ley mediante la sustitución, por la actividad de los órganos públicos, de la actividad de los particulares o de otros órganos públicos, sea al afirmar la existencia de la voluntad de la ley, sea al hacerlo prácticamente efectiva. (p.2)

Conforme comenta el autor, la actividad de los órganos públicos del Estado consiste en resolver conflictos aplicando la ley correspondiente en función a la jurisdicción que estos detentan.

Sobre la jurisdicción como garantía fundamental se comenta en González (2014):

> Si se tratara de perfilar la jurisdicción no se dejará de anotar que (i) es una garantía fundamental correlativa al derecho fundamental de acción, (ii) que (de)limita los poderes de los que está investido el órgano judicial en proceso (*gnotio*, *vocatio*, *coercitio*, *iudicium y excecutio*), (iii) implicando un contenido de garantías tanto de obrar negativo (de prohibición) como de obrar

positivo (de obligación), (iv) que efectivizan los contenidos del derecho de acción a los que se enlazan con correlatividad normativo-estructural. (p. 134)

Es decir, que la jurisdicción importa per se y difiere del proceso, diferenciándose estos conceptos según nos refiere el mismo autor.

Es importante diferenciar la garantía de jurisdicción del proceso, porque la garantía no existe por el mecanismo procedimental (*rectius est,* procesal) sino por el fin de este; de manera que el proceso como tal no es garantía, esta se encuentra en el contexto material que procura la efectividad de derechos fundamentales en el proceso y en la finalidad de este que es la sentencia. Recuérdese que la finalidad de la jurisdicción bien puede ser entendida como la solución del conflicto de intereses intersubjetivo y el logro de la paz social en justicia, fines que salen sobrando en relación al proceso porque este no soporta el alto contexto garantista de tales fines, sino, tan solo su ordenado tránsito, o mejor, su relación (*rectius est,* interacción) metódica en línea de propiciar aquello para lo que está llamado a servir: conseguir una sentencia. La desnaturalización del proceso en este orden es frecuente y no deja de tener presencia en ordenamientos procesales, v. gr., el artículo iii del Título Preliminar del Código Procesal Civil peruano.[1] (p. 127)

En relación con la jurisdicción internacional, esta tendría sus inicios con la Sentencia Serie A N° 10 del 7 de setiembre de1927 de la Corte Internacional de Justicia Permanente en el caso Lotus, nombre de la nave de pabellón francés que colisionó en altamar con una embarcación turca. En este caso Francia vs Turquía, la Corte validó la jurisdicción turca, señalando que no existía en el derecho internacional una norma que, en estos casos, estableciera la jurisdicción a favor del país de la bandera de la embarcación.

Al respecto se comenta en Stigall (2012):

[1] Código Procesal Civil. Título preliminar.
Art. 3.°. El Juez deberá atender a que la finalidad concreta del proceso es resolver un conflicto de intereses o eliminar una incertidumbre, ambas con relevancia jurídica, haciendo efectivos los derechos sustanciales, y que su finalidad abstracta es lograr la paz social en justicia. En caso de vacío o defecto en las disposiciones de este Código, se deberá recurrir a los principios generales del derecho procesal y a la doctrina y jurisprudencia correspondientes, en atención a las circunstancias del caso.

> "En esa sentencia, la Corte articuló la regla fundamental de que la jurisdicción prescriptiva - la capacidad de un gobierno para prescribir la ley relativa a ciertas actividades – es permisiva en el derecho internacional y, a menos que se demuestre una prohibición de la jurisdicción prescriptiva, un Estado puede reclamar debidamente jurisdicción."[2] (p.331)

La jurisdicción internacional se encontraría delimitada por el territorio, a decir de Velasco (2011):

> En primer lugar, hay que destacar que, desde la perspectiva del Derecho Internacional Público, la doctrina pone de relieve que el término "jurisdicción" tiene múltiples significados en función del contexto en el que se incardine el uso de dicho término. Generalmente, el vocablo describe los límites de la competencia legal de un Estado u otra autoridad normativa para aprobar, aplicar y dar cumplimiento forzoso a normas de conducta sobre las personas. (p. 11)

La afirmación sobre la jurisdicción internacional relacionada al principio de territorialidad también se comparte por Soler y Jiménez (2014):

> El denominador común de la jurisdicción internacional es la ubicación (de los hechos, las partes, las propiedades, los contratos, los agravios, etc.). Sin embargo, hay algunas diferencias entre el derecho internacional público y derecho internacional privado. Mientras que el Principio de Territorialidad determina la competencia en el derecho internacional público, en el Derecho Internacional Privado se establece por la ubicación de la parte demandada, la ubicación de la responsabilidad civil, la ubicación del acuerdo o cumplimiento contractual, la ubicación del registro de la patente o marca registrada y la ubicación del servidor. (pp. 17-18)

[2] Traducción libre al español.

Por ello la jurisdicción internacional es entendida como aquella facultad que posee el Estado para aplicar el Derecho en situaciones específicas. Mediante la jurisdicción se designa el territorio sobre el cual la potestad del Estado mismo se ejercerá, esto es, mediante los órganos competentes del mismo, en atención de la solución de los casos concretos.

La jurisdicción entendida como el poder del Estado, entonces, es exclusiva y no se ve afectada por los elementos internacionales que existan en el conflicto.

En el derecho internacional privado, la determinación la jurisdicción previamente sí pasa por un proceso donde se evalúan los factores de conexión con el foro. Estos factores, según Monroy (1995), "se encuentran en la propia relación jurídica donde se mezclan la nacionalidad, el domicilio, el *situs*, el *locus*, el *fórum*, la voluntad, etc. Son estos los denominados, en la doctrina, 'puntos de conexión'" (p. 65).

En ese sentido, conforme se señala en Delgado, Delgado y Lincoln (2002):

> "si una relación privada internacional suscita un litigio, será preciso saber: en primer lugar, cuál será el tribunal competente para resolverlo —la elección deberá efectuarse entre los tribunales de los Estados involucrados que podrían resultar competentes—, ya sea de forma alternativa o acumulativa, salvo que al respecto medie elección expresa de las partes." (p. 43)

Concluyéndose de ello que, la determinación de la jurisdicción en derecho internacional público difiere de la determinación de la jurisdicción en derecho internacional privado, la misma que se caracteriza por ser prevista por las partes, y que en caso de no existir acuerdo se analizan los puntos de conexión existentes para determinar la jurisdicción entre los Estados que resultaren involucrados, siendo esta incluso prorrogable.

1.4. El principio de Jurisdicción Universal

En virtud de la evolución del concepto de jurisdicción, dado el factor de la globalización surge el principio de jurisdicción universal, conforme se comenta en Kakowicz y Mitrani (2016):

> Las implicaciones políticas de los procesos de globalización pueden presentar nuevos problemas y desafíos políticos que provocan cambios y transformaciones en los patrones de los agentes políticos, las estructuras y las interacciones. Con todo, a final de cuentas, estos cambios y transformaciones tienen lugar bajo la autoridad de los Estados-Nación, o al menos en interacción con sus ámbitos interestatales, de manera que los agentes principales que afrontan las implicaciones de la globalización siguen siendo los Estados, tanto individual como colectivamente, según esquemas multilaterales. Argumentamos en este artículo que la política, especialmente la política interestatal, desempeña un papel crucial en nuestro esfuerzo por dar sentido a los efectos problemáticos de la globalización. También es parte vital del intento de controlar la globalización y de encontrar soluciones adecuadas a sus potenciales externalidades negativas. (p. 380)

Este fenómeno de la jurisdicción universal también ha sido definido como jurisdicción extraterritorial, según el Reporte de la Comisión de Derecho Internacional de las Naciones Unidas (2006):

> Hoy, el ejercicio de la jurisdicción extraterritorial de un Estado con respecto a personas, bienes o actos fuera de su territorio tiende a convertirse en un fenómeno cada vez más común, en gran medida como consecuencia de: (a) el aumento en el movimiento de personas más allá de las fronteras nacionales; (b) el creciente número de corporaciones multinacionales; (c) la globalización de la economía mundial, incluyendo banca internacional y bolsas de valores internacionales; (d) el aumento transnacional de las actividades delictivas, incluido el tráfico de

> drogas, el lavado de dinero, el fraude de valores y terrorismo internacional; (e) el aumento de la migración ilegal; y (f) el uso creciente de Internet a través de las fronteras nacionales con fines legales o ilegales, como los contratos electrónicos, comercio electrónico y ciberdelitos.[3] (p. 229)

Así, la globalización y el desarrollo de la tecnología son el contexto en que se da el tráfico de datos personales, planteando nuevos retos para su debida protección. Sin embargo, este principio de jurisdicción universal no se encuentra exento de críticas según señala Salmón (2007):

> La aplicación de este principio ha generado fuertes críticas, como son que la jurisdicción universal implica una intromisión en los asuntos internos del Estado que tendría competencia territorial o personal para juzgar, vulnerándose el principio de soberanía y la no intervención. No obstante, la implementación de la jurisdicción universal tiene el valor de constituir un elemento dinámico y complementario en la búsqueda de la justicia internacional, que por estar inmerso en los ordenamientos jurídicos internos de los Estados puede nutrirse de las todavía mucho más fuertes posibilidades de coerción y coacción que tienen los aparatos estatales. (p. 4)

Así, por ejemplo, los Estados Unidos de América han ejercido jurisdicción extraterritorial basada en ciertos principios de interrelación entre legislaciones nacionales y el orden legal internacional.

En ese sentido, señala Stigall (2012):

> Los tribunales de los Estados Unidos han utilizado diferentes formulaciones en abordar los desafíos al alcance de su jurisdicción. Para ello, los tribunales han abordado el problema desde el punto de vista de "cortesía", pero visto como una cuestión de obligación entre los Estados.

[3] Traducción libre al español.

> Otros tribunales han hablado de "debido reconocimiento de nuestro respeto a los propios intereses relevantes de las naciones extranjeras". Los tribunales han invocado la presunción de que el Congreso no tiene la intención de violar el derecho internacional, y palabras generales interpretadas en los estatutos de los Estados Unidos, a la luz de "las limitaciones habitualmente observadas por las naciones en el ejercicio de sus poderes". Tomadas en conjunto, estas formulaciones y las variaciones en ellas también respaldan el principio de razonabilidad como los factores establecidos con la frase de Learned Hand, que supone que tiene la intención de "castigar a todos a quienes sus tribunales pueden atrapar".[4] (p. 338)

Bajo este mismo principio de jurisdicción universal que ha sido utilizado EE.UU., la jurisdicción europea hipotéticamente podría alcanzar a los extranjeros que vulneran sus normas, más aún si para la Unión Europea la protección de datos personales es un derecho fundamental, reconocido de esta manera en su ordenamiento jurídico, pudiendo estimar ello como "justificación suficiente" para exigir el cumplimiento del mismo derecho por parte de terceros países.

[4] Traducción libre al español.

CAPÍTULO II

Protección De Datos Personales

La protección de datos personales tiene un especial desarrollo en la doctrina, jurisprudencia y legislación europea.

Sin bien el derecho a la protección de datos personales se ha vinculado con los derechos a la privacidad, intimidad y dignidad del individuo, la protección de datos personales resulta más amplio que los mencionados derechos.

De esta manera señala Martínez-Martínez (2018):

> El objeto del derecho a la protección de datos es más amplio que el derecho a la intimidad (art. n.° 18.1 de la Constitución española), afectando a la esfera de otros bienes de la personalidad como la dignidad personal, el honor y el pleno ejercicio de los derechos de la persona, de tal forma que su protección no se reduce solo a los datos íntimos sino también: "a cualquier tipo de dato personal, íntimo o no, cuyo empleo o conocimiento por tercero pueda afectar a sus derechos". (p. 188)

El derecho a la protección de datos personales también es entendido como el derecho de autodeterminación informativa.

El derecho de autodeterminación informativa ha sido desarrollado jurisprudencialmente, por el Tribunal Constitucional español en la sentencia 292/2000, del 30 de noviembre de 2000, conforme se reseña en Orrego (2013):

> El derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico

> ilícito y lesivo para la dignidad y derecho del afectado […] atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. (p. 320)

El derecho a la protección de datos personales concebido como un derecho de autodeterminación informativa es objeto de garantía bajo las normas previstas en el marco del RGPDUE.

2.1 **Datos Personales**

Sobre la noción de "datos personales", se reseña en Gutiérrez (2012):

> Ese término es utilizado para designar cualquier información relativa a un sujeto identificable. Merece destacarse que su ámbito es muy amplio, ya que incluye no solo la información descriptiva básica (como el nombre, la edad, el género, el color de pelo) sino también cualquier otra información sobre el individuo. La información puede ser tan diversa como la relativa al paradero de la persona, sus hábitos alimenticios, la propiedad de un vehículo u otras propiedades, su dirección postal o de e-mail, su número de teléfono, el desarrollo de su trabajo, estado de salud, opiniones, intenciones y otros aspectos de su personalidad. En el ámbito particular del proceso penal, los datos personales pueden referirse también a sus antecedentes penales, huellas dactilares o perfil de ADN. (p. 51)

Atendiendo a lo señalado por el citado autor acerca de los datos personales, se advierte que estos son todos aquellos por los cuales se guarda cierta información personal que puede

ser relevante para la protección del derecho a la intimidad y otros conexos. De ahí la necesidad de su respeto a nivel internacional.

Respecto al derecho a la intimidad, podemos citar la definición esbozada por Meján (1996):

> La intimidad es el conjunto de circunstancias, cosas, experiencias, sentimientos y conductas que un ser humano desea mantener reservado para sí mismo, con libertad de decidir a quién le da acceso al mismo, según la finalidad que persiga, que impone a todos los demás la obligación de respetar y que solo puede ser obligado a develar en casos justificados, cuando la finalidad perseguida por la develación sea lícita.

Sobre el derecho de protección de datos personales, en relación con el derecho a la intimidad, Guzmán (2013), indica:

> La protección de datos personales es un derecho fundamental relativamente nuevo, y configurado a partir de las concepciones que se tienen de la vida privada o intimidad, del derecho al honor y del derecho a la propia imagen. La evolución de estos derechos, principalmente el de la vida privada, han planteado nuevas situaciones que habrán de ser motivo de la creación de un nuevo derecho, la protección de datos personales. (p. 112)

Si bien, la protección de los datos de las personas tiene por finalidad salvaguardar la intimidad y privacidad de las mismas, el derecho de protección de datos es un derecho autónomo e independiente del derecho a la intimidad y privacidad. Este derecho incluso puede considerarse de mayor envergadura, ya que se caracteriza por poner de relieve el conocimiento, consentimiento e imperio de las personas en relación con el acceso y utilización de sus datos, conforme se analizará en el siguiente acápite.

2.2. **Tratamiento de Datos Personales**

Sobre el tratamiento de los datos personales, Gonzáles (2016) señala que:

> Es cierto que, para que se hable de tratamiento de datos de carácter personal, estas informaciones deben ser almacenadas o conservadas, por lo que para que esto se produzca habrá que extraer los datos de la fuente de información (acceso) y tratar o utilizar el dato. Esta acción permite diferenciar el mero acceso a un dato del tratamiento que pueda efectuarse a posteriori. Por ejemplo, la simple recepción de un CV sin que se conserven los datos contenidos en él no sería un tratamiento de datos. (p. 67)

Refiriere Gonzáles (2016) que, el tratamiento de datos personales conlleva un desafió en el contexto de la globalización, comentando que "los retos que propone el derecho fundamental a la protección de los datos personales exceden las tradicionales fronteras de los Estados e incluso de zonas geográficas completas, y se instala como un problema global en un mundo interdependiente" (pp. 349-350).

Sobre los retos de la protección de derechos fundamentales en un mundo globalizado, también se comenta en Poschl (2015):

> La bipolaridad de la relación de derechos fundamentales —a un lado el ciudadano, a otro el Estado— ha pasado, en primer lugar, a ser una pluralidad multipolar, de suerte que junto al Estado aparecen bajo el foco, como sujetos de una posible injerencia sobre los derechos fundamentales, híbridos privado-estatales, poderosos actores privados y figuras difusas como las comunidades de internet. Esta ampliación de los sujetos que intervienen sobre los derechos fundamentales se corresponde, en segundo término, con la extensión y descentralización de los instrumentos de poder, que, como antes, se sigue ejerciendo a través de la coacción, pero también con el dinero

> y, sobre todo, mediante la información. En tercer lugar, se han diversificado los lugares desde los que producen injerencias en los derechos fundamentales: el escenario es hoy el mundo entero. (p. 127)

En un escenario con multiplicidad de actores y transferencias simultaneas de datos en línea, el tratamiento de datos personales representa un gran desafío. Sobre el contenido y alcances del tratamiento de datos, el Reglamento General de Protección de Datos de la Unión Europea del 27 de abril de 2016 (artículo 4.2) señala que este consiste en:

> "Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción."

De esta regulación podemos colegir que la información clara, precisa y efectiva debe preceder al consentimiento de las personas para que este sea considerado válido. En virtud de que el tratamiento se da sobre los datos de las personas, resulta vital la relación del consentimiento con el ejercicio de la autonomía y la voluntad de las mismas, por ser este de carácter personalísimo.

Respecto de esta autonomía, esencia del derecho a la autodeterminación informativa se comenta en Moya (2010):

> Es esencial otorgar a las personas autonomía sobre su consentimiento en cuanto a la posibilidad de autorizar, bloquear, oponerse, rectificar la información que está circulando a su respecto, lo que se configura en una autodeterminación informativa, definiendo la facultad del individuo de

decidir básicamente por sí mismo cuándo y dentro de qué límites procederá a revelar situaciones concernientes a su vida privada. (p. 60)

Ahora, si bien hemos señalado la importancia del derecho a la protección de datos personales, no debemos soslayar derechos que, en ocasiones, pueden entrar en conflicto con el mismo, que han sido invocados en muchos casos judiciales, y que también son considerados como derechos fundamentales por la Unión Europea, como lo son la libertad de expresión e información.

2.3. **Legislación de la Unión Europea sobre Protección de Datos Personales**

La Unión Europea consagra el derecho de protección de datos como un derecho fundamental, según su Carta de Derechos Fundamentals (2000/C 364/01) proclamada en la Cumbre de Niza, con fecha 07 de diciembre del 2000, señalando en su artículo 8° lo siguiente:

Artículo 8.°. 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 recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Cabe señalar, además, que este derecho se consagra como un derecho fundamental independiente del Respeto a la Vida Privada y Familiar, preceptuado en el artículo 7.° de la Carta de los Derechos Fundamentales de la Unión Europea, que establece que “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”.

Sin embargo, con anterioridad al reconocimiento de este derecho como derecho fundamental por la Unión Europea, la protección de datos personales se encontraba regulada en la Directiva 95/46/CE, del 24 de octubre de 1995, sobre esta normativa comenta Gacitua (2014):

> "Al momento de elaborarse la Directiva 95/46/CE, **no existía la carta de Derechos Fundamentales de la Unión Europea** y, por tanto, el derecho a la protección de datos personales no se había reconocido aún como un derecho fundamental autónomo en el Derecho Originario ni Derivado de la Unión Europea. Es por ello que los artículos y considerandos de la Directiva hacen referencia indistintamente al derecho a la intimidad y al derecho al respeto de la vida privada reconocido **en el artículo 8.° del convenio europeo para la protección de los derechos humanos y de las libertades fundamentales**, así como en los principios generales del Derecho comunitario, como soporte *ius* fundamental de la directiva". (p. 176)

La directiva 95/46/CE es una normativa de gran relevancia para el derecho de la Unión Europea, conforme añade Gacitua (2014):

> La directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, tiene por objeto establecer normas relativas 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, la directiva 95/46/CE). Este instrumento es la pieza fundamental dentro del derecho derivado europeo en materia de protección de los datos personales […]. De esta forma, la directiva 95/46 viene a aproximar las legislaciones nacionales de los Estados Miembros de la Unión Europea en cuanto al derecho a la protección de datos personales, convirtiéndose hasta la actualidad en el principal instrumento normativo europeo de legislación derivada relativo a la protección de datos. (pp. 174-175)

Actualmente, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, vigente a partir del 25 de mayo del 2018, cuerpo normativo en que se ampara el Derecho Fundamental a la Protección de Data de Carácter Personal, viene a reemplazar la Directiva 95/46/CE.

2.4. **El enfoque de los Estados Unidos de América sobre Protección de Datos Personales**

Una de las cuestiones que se analiza en el presente trabajo, es el enfoque de la protección de datos personales en los Estados Unidos de América.

En principio, destaca la conducta autorregulatoria del mercado que se privilegia en los EE.UU, conforme se recoge en el documento elaborado por la Comisión de Asuntos Jurídicos y Políticos del Consejo Permanente de la Organización de los Estados Americanos del 03 de abril del 2012, donde se hace referencia a las medidas que sigue EE. UU. en cuanto al tratamiento de los datos personales, adoptado en el marco de la APEC (*Asia Pacific Economic Cooperation*):

> El 13 de noviembre de 2011, el presidente Obama y los representantes de los países integrantes del APEC avalaron el Sistema de Reglas Transfronterizas sobre Privacidad, en una reunión en Honolulu, Hawai. Se trata de un código de conducta autorregulatorio encaminado a crear un sistema de protección más uniforme para los consumidores cuando sus datos son transferidos de un país a otro en la región del APEC, con diferentes regímenes. Las compañías que deseen participar en este sistema del APEC tendrán que pasar por un proceso de revisión y certificación a cargo de terceros, que examinarán sus políticas y prácticas de privacidad y velarán por la implementación de las nuevas reglas. (p. 76)

Esta referencia al libre mercado y autorregulación del mismo que prima en los EE.UU, se comenta también en Peltz-Steele (2015):

> La obsesión de los Estados Unidos con la libertad económica explica el enfoque persistente en las relaciones comerciales desde *Safe Harbour 2000* hasta la Declaración de Derechos de Privacidad del Consumidor 2015. Las relaciones entre personas y actores comerciales en los Estados Unidos son cuestiones de contrato y propiedad. El paradigma del secreto surge de la noción de datos personales como propiedad. En el derecho común, una persona no tiene un persistente interés jurídico en la propiedad que se vende o se regala. Además, un derecho constitucional de reedición pesa fuertemente en contra de la regulación de divulgación o transferencia de información. Los actores públicos solo pueden ser regulados por el funcionamiento negativo de la ley constitucional o estatutaria. Un procesador de datos opera bajo una presunción de permisibilidad, sujeto a restringidas limitaciones. (p. 20)

Dado el contraste con el enfoque humanista del derecho fundamental de protección de datos de la Unión Europea, el gobierno de los EE.UU., en aras de mantener la dinámica del comercio con la Unión implementó el sistema de *Safe Harbour*.

Ewing (2002) nos indica "el puerto seguro está diseñado para crear una presunción de adecuación para las organizaciones estadounidenses que reciben datos personales de Naciones europeas"[5] (p.338).

No obstante, conforme comentaremos más adelante, el TJUE, mediante sentencia del 8 de febrero de 2012 (Recurso n.° 25/2008), conocida como la sentencia Scherms declaró la nulidad del sistema *Safe Harbour* por considerarlo no garantista de la protección de datos personales.

Es así que la brecha entre Europa y EE. UU., por la diferencia de su regulación en materia de protección de datos, en el primero, y de autorregulación, en el segundo, se hace más

[5] Traducción libre al español.

profunda en relación con los avances en materia de protección de datos personales de la Unión Europea.

El enfoque americano sobre la protección de datos personales es comentado también por Ornelas Núñez e Higuera Pérez (2013):

> En aparente oposición al modelo europeo se encuentra el modelo sectorial-autorregulatorio de protección de datos adoptado por los Estados Unidos de América. Este modelo se basa en la creencia de que la regulación excesiva por parte del gobierno inhibe el desarrollo de la economía, y que el mercado es capaz de autorregularse en la materia, siempre y cuando haya un interés real de los consumidores, como en el caso de la confianza necesaria para realizar compras a través del comercio electrónico. (pp. 8-9)

Es por ello que, se afirma que la Unión Europea cuenta con una legislación severamente más estricta de privacidad de datos, mientras que, para los EE. UU., las leyes de protección de datos permiten que estos sean más accesibles por el mundo exterior en virtud del dinamismo del comercio que dicho Estado procura.

El efecto práctico de los enfoques comparados determinaría que las empresas estadounidenses pudieran estar cumpliendo con sus estándares de tratamiento en EE. UU., que privilegia el dinamismo del mercado, pero estos estándares podrían no ser necesariamente coincidentes con la regulación de la Unión Europea en materia de protección de datos personales.

Al ser el RGPDUE, una regulación que entró en vigencia el 25 de mayo de 2018, los reales efectos no se han observado aún, pues si bien para las autoridades europeas el ideal sería la protección de los derechos de sus ciudadanos, incluso fuera de sus fronteras, los controles podrían afectar el dinamismo del comercio y el tráfico digital con otros países.

2.5. **Derecho a la información y libertad de expresión en relación con el Derecho de Protección de Datos Personales**

La protección de datos personales de la Unión Europea no implica el desconocimiento de los derechos a la información, también reconocidos en su Carta de los Derechos Fundamentales. Es así que, en el RGPDUE 2016/679 del 27 de abril de 2016 (Considerando 4), se señala que:

> El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

En ese sentido, podemos concluir en que las diferencias de las regulaciones analizadas se deben a la existencia de un desacuerdo, incluso una contraposición, entre los ideales de ambos: por un lado, el enfoque humanista y la preeminencia de los derechos fundamentales en Europa y, por otro lado, el enfoque capitalista, que se basa en el principio de libertad personal y económica, así como en el carácter constitucional del derecho a la información.

En cuanto al derecho a la información, Soto (2010), dentro de su investigación, menciona lo siguiente:

> Varios autores coinciden en que, el derecho de la información nace, precisamente, de la llamada sociedad de la información, que surge de los significativos avances tecnológicos en medios de

> comunicación dados en las últimas décadas. La trasformación de la también llamada sociedad del conocimiento obedece al fenómeno de la rápida y masiva transmisión de datos, que se puede llevar a cabo por diversos medios. Quedando inmersa en un mundo de posibilidades para allegarse de información de diversos temas y lugares. La necesidad que experimenta esta sociedad, de obtener información actual y de diversa índole, es lo que la distingue y la denomina como tal. Condición que trae consigo la necesidad de regular la actividad informativa y todos los fenómenos que de esta se generen, como lo mencionan algunos autores, dando origen al denominado Derecho de la Información. (p. 30)

No obstante, el Reglamento General de Protección de Datos emitido por la Unión Europea contrasta por su reforzamiento de los derechos de las personas y la autonomía en relación al tratamiento de sus datos, así como la exigencia de precisión, exactitud y oportunidad de la información previa, que debe brindarse para que las personas manifiesten su consentimiento, limitando, a su vez, las excepciones a estos derechos[6], conforme se expone en el siguiente capítulo.

[6] En dicho contexto, el RGPD ha previsto estos derechos de libertad de expresión e información como excepciones al Derecho al Olvido (artículo 17.°), así como excepciones al tratamiento de los datos (artículo 85.°), y también ha armonizado los mencionados derechos con la regulación que establece para la consideración de la Licitud del Tratamiento (artículo 89.°).

CAPÍTULO III

Reglamento de Protección de Datos Personales de la Unión Europea y sus implicancias

Según el Reglamento General de Protección de Datos de la Unión Europea (2016/679, artículo 4.1), los datos que protege esta normativa están referidos a:

> 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, uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

En el presente capítulo trataremos sobre el RGPDUE, sus implicancias y las consecuencias que trajo consigo su entrada en vigencia.

3.1. **De las sanciones previstas en el RGPDUE**

¿Cuáles serían las posibles sanciones y consecuencias ante el incumplimiento de la normativa bajo análisis, según el actual Reglamento General de Protección de Datos?

En resumen, según la revista Expansión (2018):

Tenemos que estas sanciones se pueden dividir en dos bloques:

- Sanciones Graves. Comprende sanciones hasta 10 millones de euros o el 2 % del volumen total anual global de la facturación del año anterior.
- Sanciones Muy Graves. Comprende las sanciones hasta 20 millones de euros o el 4 % del volumen total anual global de la facturación del año anterior.

Ahora bien, en relación con las multas impuestas por las Autoridades Europeas ante el incumplimiento de la normativa de protección de datos vigente hasta el 24 de mayo de 2018, se cita a Sánchez, J. (2018):

> La Agencia Española de Protección de Datos (AEPD) ha impuesto la mayor sanción económica a *Facebook* y *WhatsApp* por la cesión de información sensible.
>
> El regulador español, según el dictamen emitido este jueves, da por probada la existencia de dos infracciones graves de la Ley Orgánica de Protección de Datos. Así, ha multado a cada una de las empresas con 300.000 euros, la cuantía máxima correspondiente a las infracciones graves declaradas: una de ellas directamente a la aplicación de mensajería instantánea por "comunicar datos a Facebook sin haber obtenido un consentimiento válido de los usuarios" y otra a la empresa matriz "por tratar esos datos para sus propios fines sin consentimiento".

De otro lado, la mayor sanción impuesta por incumplimiento al RGPDUE la establecida por la Comisión Nacional de Informática y Libertades de Francia-CNIL, en la deliberación SAN-2019-001 del 21 de enero de 2019, que pronuncia una sanción financiera contra *Google LLC* de 50 millones de euros.

Según el fundamento 97 de la resolución, el Comité Restringido consideró que el diseño general de la información elegida por *Google* no cumplía con los requisitos del Reglamento, en particular con lo establecido en el artículo 13.°[7] del RGPDUE. En tanto, la información que

[7] Artículo 13.°. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.
1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; L 119/40 ES Diario Oficial de la Unión Europea 4.5.2016;
d) cuando el tratamiento se base en el artículo 6.°, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46.° o 47.°, o el artículo 49.°, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas, o al hecho de que se hayan prestado.

Google comunicaba a las personas se extendía a varios documentos: "Política de privacidad y Términos de servicio", que se muestran durante la creación de una cuenta, y luego los "Términos de servicio" y "Política de privacidad", a la que se puede acceder posteriormente a través de enlaces clicables en el primer documento.

El Comité también señaló que la configuración de personalización de la cuenta, que contiene la opción de mostrar publicidad personalizada, se verifica previamente de forma predeterminada, lo que significa, a menos que se indique lo contrario, el consentimiento del usuario para procesar sus datos para los fines mencionados (p. ej., historial de búsqueda de *YouTube*, visualización de publicidad personalizada, etc.). El usuario tiene la opción de desmarcar esta configuración si no desea que se implemente este procesamiento.

En vista de lo anterior, se concluyó que, aunque el usuario tiene la posibilidad de cambiar la configuración de su cuenta antes de su creación, es necesaria una acción positiva de su parte para acceder a las opciones de configuración de la cuenta. El usuario puede crear completamente su cuenta y aceptar el procesamiento relacionado, incluido el procesamiento de publicidad personalizado, sin hacer clic en "Más opciones".

Para la autoridad, el consentimiento del usuario, en este caso, no se recababa de manera válida, ya que no se otorga a través de un acto positivo por el cual la persona consiente específicamente y por separado el procesamiento de sus datos con fines de publicidad personalizada, en oposición a otros fines de procesamiento.

El Comité Restringido consideró que, a la luz de las características particulares de este procesamiento de datos personales, las características "claras" e "inteligibles", en el sentido del artículo 12.°[8] del RGPD, de la información referida en el Reglamento, no se respetaban en el caso analizado.

(…).

[8] Artículo 12.°. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13.° y 14.°, así como cualquier comunicación con arreglo a los artículos 15.° a 22.° y 34.° relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular

Además de ello, en la deliberación SAN-2019-001 del 21 de enero de 2019, se señala que, "modificar las preferencias de usuario, a menudo hace necesario navegar por diversos menús que, además, muestran opciones de recolección de datos activadas por defecto". "Este tipo de procedimiento lleva al usuario a dar su consentimiento global, pero el consentimiento no es 'específico' como se requiere en la GDPR".

Además de las sanciones económicas comentadas, las compañías corren un riesgo reputacional, conforme se comenta en Wimmer 2018 (p. 2) respecto de que, "aparte de las consideraciones legales, puede haber importantes problemas de reputación y prácticos que surjan al resistir un pedido bajo el RGPDUE que las compañías tomarán en consideración".

En ese sentido, se prevé que las grandes empresas alinearían sus prácticas en materia de protección de datos a lo que señala el Reglamento, no obstante, los costos de transacción que ello implique, así como el consentimiento expreso, que requiere esta normativa, que al implicar costos de transacción pueden afectar el dinamismo del mercado, conforme se hará referencia más adelante.

3.2. **La Protección de Datos Personales en la UE y la Protección al Consumidor en EE. UU.**

La comprensión y adaptación de la regulación europea en materia de protección de datos representa un gran desafío para las empresas americanas, en tanto, las principales empresas de tecnología se encuentran constituidas en los EE. UU.

cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.
(…).

En el "Debate sobre Privacidad y Seguridad en la Red: Regulación en los Mercados",[9] que tuvo lugar en el año 2012, fueron analizadas las diferencias que se han venido comentando, en las opiniones intercambiadas entre los especialistas europeos y americanos en el marco del desarrollo y publicación del proyecto del Reglamento de Protección de Datos de la Unión Europea, donde se hizo énfasis, por el lado europeo, en la prevalencia del derecho fundamental a la protección de datos, mientras que por el lado de los EE. UU. se expresó la preocupación por la posible incompatibilidad de la regulación con los derechos a la libertad de información y los sobrecostes para las empresas estadounidenses que tienen operaciones con Europa.

Esta diferencia ha quedado reflejada a través de un sonado caso, que tuvo lugar, coincidentemente, en el contexto en que se encontraba próxima la entrada en vigencia del RGPDUE.

El caso denominado *Cambridge Analytica* y la masiva fuga de datos que afectó a millones de usuarios de *Facebook*, pareciera haber puesto de relieve la importancia de la protección de datos personales. Siendo que incluso el Parlamento Europeo tuvo la oportunidad de citar a declarar al CEO de la compañía americana *Facebook*, que ofrece servicios de redes sociales a nivel global.

¿De qué trata el caso *Cambrige Analytica*? Este es el nombre de la consultora que estuvo involucrada en la campaña para las elecciones presidenciales de EE. UU. del año 2016, a la que se la acusa de manipular datos de 50 millones de usuarios de *Facebook*.

Dice De Llano (2018):

> Una investigación conjunta de *The New York Times* y *The Observer* revela que, en 2014, la compañía se hizo con una base de datos de pretendido uso académico y la explotó sin permiso para elaborar estrategias electorales durante las elecciones intermedias en Estados Unidos. Se

[9] Obra que reúne las contribuciones de los expertos más relevantes del mundo académico y empresarial de Europa y Estados Unidos de América.

trata de uno de los mayores hurtos de información de la historia de *Facebook*. Dos años después, *Cambridge Analytica*, que todavía estaba en posesión de ese ingente material, dio servicio a la candidatura presidencial del republicano Trump, que ganó las elecciones de noviembre de 2016.

La mencionada cifra de afectados, en realidad, habría sido mucho mayor, al precisar *Facebook*, a través de su director de Tecnología, *Mike Schroepfer*, que, luego de las investigaciones que tuvieron lugar por parte de la propia compañía, en total fueron 87 millones de personas las afectadas. "En total, creemos que la información de *Facebook* de hasta 87 millones de personas, principalmente en los EE. UU., puede haber sido compartida de forma incorrecta con *Cambridge Analytica*".[10] (Newsroom.fb.com 2018)

En ese contexto, el Senado y el Congreso de Estados Unidos citaron a *Mark Zuckerberg*, CEO de *Facebook*, para que responda una serie de cuestionamientos sobre la filtración de los datos de millones de personas, encuentros que tuvieron lugar los días 10 y 11 de abril de 2018, respectivamente, mientras se venía redactando el presente trabajo.

En el marco del debate antes señalado, en la Cámara de Senadores de EE. UU., en una audiencia transmitida en vivo alrededor del mundo, la senadora María Cantwell cuestionó a *Zuckerberg* en relación con la aplicación de la regulación europea en Estados Unidos,[11] haciendo referencia al RGPDUE.

El CEO de *Facebook* señaló que, independientemente de si en los EE. UU. se implementa o no la aludida reglamentación, su compañía viene implementando la misma, en cuanto a los

[10] Traducción libre al español.

[11] Anónimo (2018): Comparecencia de *Marck Zuckerberg* ante el Senado de EE. UU. (10/04/2018). Cantwell: "¿Cree que las regulaciones europeas deberían aplicarse aquí en los EE. UU.?" *Zuckerberg*: Senadora, creo que todos en el mundo merecen una buena protección de privacidad. Independientemente de si implementamos exactamente la misma regulación, supongo que sería algo diferente, porque tenemos sensibilidades algo diferentes en los EE. UU., como en otros países. Nos comprometemos a extender los controles y el consentimiento afirmativo y los controles especiales en torno a tipos de tecnología delicada, como el reconocimiento facial, que se requieren en el RGPD. Estamos haciendo eso en todo el mundo. Por lo tanto, creo que vale la pena discutir si deberíamos tener algo similar en los EE. UU. Pero lo que me gustaría decir hoy es que vamos a seguir adelante y ponerlo en práctica, independientemente de cuál sea el resultado reglamentario. (*Washington Post*, 2018).

controles, consentimiento y herramientas como el reconocimiento fácil, pero él supone que en su país esta regulación podría ser algo diferente, en atención a que en los EE. UU. se tienen diferentes sensibilidades sobre este tema, al igual que en otros países.

En virtud de este conocido caso, parece ser el mundo se ha percatado de la gravedad de las consecuencias del indebido tratamiento de datos personales.

Sin embargo, a pesar de la reacción que los legisladores de los EE. UU. mostraron frente a *Facebook* y el caso *Cambridge Analytica*, hasta la fecha no se ha legislado en una línea similar a la de Europa en relación con la protección de los datos personales. Esta apreciación se comenta en el portal web de negocios, economía, finanzas y tecnología *Quartz*, donde se critica la actuación de los legisladores, al advertir que es muy poco probable que estos favorezcan una estricta regulación.

Koslowka y Timmons (2018):

> Algo que quedó muy claro durante el interrogatorio a *Zuckerberg*: los legisladores estadounidenses no quieren o no pueden forzar leyes para proteger la privacidad de los datos de los estadounidenses, y mucho menos intentar hacer que la empresa que ganó $ 16 mil millones al año redefina radicalmente su modelo de negocios, incluso después de que este caso fue armado por los rusos para influir en las elecciones estadounidenses [...].
>
> "En el pasado, muchos de mis colegas de ambos lados estaban dispuestos a ceder a los esfuerzos de las compañías tecnológicas para regularse a sí mismos", "pero esto puede estar cambiando", indicó el senador republicano Jhon Thune, de Dakota del Sur. Declaración que más parece una solicitud de permiso a *Zuckerberg* para que aprobara la reglamentación en lugar de servir como el organismo legislativo de los EE. UU.

Las autoridades de EE. UU. preferirían no regular estas actividades y dejar que el mercado lo haga. Ello podría tener sentido, en virtud de que, como señala Broseta Pont (2005:

55), “desde finales de los ochenta hasta la actualidad se asiste a un nuevo resurgir de las ideas neoliberales en lo económico, que se traduce en la reducción drástica de la intervención del Estado como agente económico directo (privatización de empresas públicas) y, sobre todo, en una progresiva reducción de los sectores regulados (desregulación) y un generalizado incremento de la competencia”, hecho que, como explica el autor, no supone que el Estado deje de lado su importante papel regulador de las actividades económicas, pero se considera que se hacen más limitadas a ciertos sectores, enfocando su regulación a sectores clave, por ejemplo, la explotación de recursos naturales que compete y afecta el medio ambiente y por ende resulta de interés público, de la misma manera que a otros sectores de la economía, como la energía.

Con un enfoque diferente, en razón de los hechos ocurridos en el caso *Cambridge Analytica*, la Comisión Federal de Comercio de EE. UU. (FTC por sus siglas en inglés) ha aplicado la mayor sanción impuesta a una compañía americana por la suma de 5 billones de dólares, en virtud de que *Facebook*, habría vulnerado un acuerdo previo del año 2012, donde se comprometió a no infringir normas de protección al consumidor.

Al respecto, comenta Fair (2019):

> La orden de la FTC del 2012 estableció penalidades por si *Facebook* hacía declaraciones engañosas en el futuro sobre el control de los consumidores sobre la privacidad de su información personal.
>
> De acuerdo a la FTC, eso es justo lo que sucedió. *Facebook* violó la orden al, nuevamente, darle acceso a compañías a la información de consumidores que dijeron que no querían compartirla. La FTC también alega que *Facebook* hizo otras declaraciones engañosas sobre cómo usaba la tecnología de reconocimiento facial, los números de teléfono celular de los consumidores y otros datos personales.

Finalmente, y tal como la compañía había estimado, efectuando una provisión significativa frente a esta contingencia, sus representantes suscribieron un millonario e histórico acuerdo, por el que *Facebook* se obligó a pagar una penalidad de $ 5 mil millones de dólares a favor del gobierno americano. Asimismo, *Facebook* se comprometió a transparentar las prácticas sobre la privacidad de los consumidores y a establecer un comité independiente dentro de su Directorio que intervendrá en las decisiones sobre privacidad, entre otras medidas que buscan proteger la privacidad de los usuarios.

EE. UU. habría optado por imponer sanciones drásticas desde la perspectiva de publicidad engañosa al consumidor y dar un severo ejemplo a las empresas a través de la penalidad impuesta a *Facebook*. No obstante, este mecanismo o situación dista mucho del reconocimiento general como derecho fundamental a la Protección de Datos Personales de la Unión Europea, a pesar de que en ambos casos el derecho que subyace es el derecho a la privacidad y la autodeterminación informativa.

En efecto, como venimos comentando, la aplicación extraterritorial de la normativa europea que surge en el contexto de la globalización de las comunicaciones y del avance tecnológico en un ciberespacio que no tiene espacio ni fronteras posee diferentes matices y enfoques sobre los derechos involucrados, generándose una falta de consenso en este ámbito.

3.3. **De la extraterritorialidad del Reglamento de Protección de Datos de la Unión Europea**

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 indica en su artículo 3.º, con relación a su ámbito de aplicación:

> 1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.
> 2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

De lo señalado en el RGPDUE se había entendido que esta normativa prevé un alcance extraterritorial con la finalidad de garantizar la protección de su objeto, esto es, el respeto del derecho fundamental de la protección de datos de carácter personal.

Este pretendido alcance extraterritorial de la normativa de protección de datos tiene lugar en un contexto de aceleración en el desarrollo de las comunicaciones y la tecnología que han trastocado el concepto de territorio.

En ese sentido, la limitación geográfica tradicional, era entendida como "el territorio", según se señala en Pérez y Wieland (2007):

> El territorio es la base física o espacial sobre el cual un Estado ejerce su autoridad y por lo tanto sus poderes y competencias. En buena cuenta, el territorio es el soporte material necesario para la existencia del Estado, ya que este ejerce sobre aquel su soberanía. Cuando hablamos de territorio del Estado se hace referencia a una triple realidad: por territorio se entiende tanto el espacio terrestre independiente de su extensión como el espacio terrestre y sometido a la soberanía del Estado, así como el espacio aéreo superpuesto a los dos espacios anteriores. (p. 277)

El territorio, entonces, se enmarcaba en la Teoría del Estado como aquel elemento físico sobre el cual se desenvuelve una nación, es decir, se mostraba como la base espacial que otorga el acondicionamiento perfecto para que este Estado ejerza su soberanía, entendida como el poder o conjunto de facultades que este detenta en vista de la organización y comunidad social.

El principio de territorialidad, no obstante, ha perdido sentido en el contexto actual, a decir de Soler y Jiménez (2014): "La razón principal de los problemas de regulación de Internet es que las leyes y reglamentos se han creado bajo el supuesto de que las actividades están geográficamente localizadas y, en consecuencia, la ubicación es el criterio para determinar la jurisdicción y competencia". (p.16)

En efecto, conforme hemos venido comentando, en el mundo en el que vivimos, donde predomina la tecnología y, la información fluye de manera dinámica y exponencial, el concepto de extraterritorialidad pareciera cobrar mayor relevancia, y presenta la problemática que reseñamos a continuación.

3.3.1 **De la extraterritorialidad del RGPDUE y su problemática**

Surge, la interrogante sobre el análisis y aplicación de las normas previstas en el RGPDUE fuera del territorio de la Unión Europea. De otro lado, la cuestión sobre el reconocimiento y/o ejecución fuera de su territorio de una sentencia emitida por un Tribunal Europeo que hubiera determinado una sanción por infracción al RGPDUE a una empresa situada fuera de su territorio.

Estimo que, en el caso de las autoridades de EE. UU. pudieran no reconocer una sentencia[12] proveniente de la Unión Europea en materia de Protección de Datos Personales, en

[12] En los EE. UU., todos los estados tienen la obligación constitucional de dar fe pública a las sentencias dictadas en otros Estados, pero las sentencias de tribunales extranjeros solo se aplican sobre la base de la cortesía. Por regla general, los tribunales norteamericanos conceden el Exequátur de sentencias extranjeras en aquellos casos en que en la tramitación del

tanto, no reconocen en su sistema jurídico, la protección de datos personales como derecho fundamental.

Al respecto, señala Parrish (2008):

> Esto es particularmente cierto cuando los Estados Unidos aplican un doble estándar: permitir que los extranjeros sean demandados en los tribunales estadounidenses, pero no permitiendo que se presenten demandas de derechos humanos contra los actores estadounidenses. En consecuencia, la aplicación vigorosa de los derechos humanos a través de instrumentos e instituciones internacionales, a menudo, tiene un mayor reclamo de legitimidad que la aplicación interna. Existen pocas razones para creer que las leyes extranjeras necesariamente sean consistentes con los conceptos occidentales de justicia. (pp. 866-867)

Se advierte por tanto, un posible dilema en relación con el principio de universalidad de los derechos fundamentales, según se explica en Vargas (2015: 1): "A pesar del reconocimiento de la universalidad de los Derechos Humanos, así como de la participación de la gran mayoría de los países en el Sistema Internacional de los Derechos Humanos, los Estados tienden a limitar su responsabilidad al interior de sus propias fronteras, lo que implica un vacío en la protección real de los derechos a nivel internacional". Esta situación de jurisdicción territorial se contradice, pues, con el compromiso que deberían tener los Estados de respetar los derechos fundamentales a nivel global.

Ante ello, surge la pretendida extraterritorialidad de la norma en cuestión, conforme se comenta en Alfu (2018):

procedimiento de instancia en el país extranjero se hayan respetado las garantías constitucionales que inspiran los principios de la tutela judicial efectiva. Sin embargo, no siempre es así. Existen precedentes denegatorios de Exequátur por una amplia variedad de razones distinta de la vulneración de la tutela judicial efectiva y que incluyen desde la concurrencia de defectos formales o planteamientos procesales inadecuados hasta causas más sustanciales como, por ejemplo, la vulneración del orden público norteamericano y de sus derechos constitucionales. (Varela 2016: p.237).

El campo de aplicación cubrirá no solo a entidades que traten datos de carácter personal que se encuentren dentro del territorio europeo, sino también a empresas o entidades del mundo entero que traten datos personales como parte de las actividades de una de sus sucursales establecidas en la UE, independientemente del lugar donde sean tratados los datos; o empresas establecidas fuera de la UE que ofrecen productos o servicios (de pago o gratuitos), u observan el comportamiento de los ciudadanos o residentes de la UE.

En el mismo sentido, refiere Espinosa (2018):

A mayor abundamiento, el RGPDUE tiene un ámbito de aplicación extra-territorial, en el que dicha regulación es aplicable a cualquier persona o compañía que: trate datos personales de cualquier ciudadano europeo, o dirija su publicidad o servicios a ciudadanos europeos, aunque su domicilio no esté físicamente en Europa; o que teniendo su domicilio en Europa trate datos personales, sin importar que el tratamiento de estos no se realice en Europa o los titulares de los datos no sean europeos.

Otras opiniones, incluso han graficado los supuestos de hecho para la aplicación del RGPDUE; así uno de los jurídicos más prestigiosos de Londres, Reino Unido[13], Slaughter y May (2018) señalan que la normativa europea alcanzaría a:

1) Empresas no establecidas en la Unión Europea pero que ofrezcan servicios a individuos en ella, vía un *website* ubicado fuera del territorio de la Unión.

[13] A la fecha de promulgación y vigencia del RGPDUE, el Reino Unido formaba parte de la Unión Europea. El 31 de enero de 2020 se cumplió el plazo estipulado para su salida. Durante los próximos once meses, el Reino Unido deberá negociar los nuevos términos de su relación con la Unión Europea. (Fuente *BBC News*: "Qué es el Brexit y otras 5 preguntas básicas para entender la salida de Reino Unido de la Unión Europea").

2) Empresas no establecidas en la Unión Europea pero que utilizan *cookies* para rastrear a clientes pasados (clientes de la Unión Europea) que navegan buscando, por ejemplo, hoteles en un determinado destino.

3) Empresas de *delivery* o distribución no establecidas en la Unión Europea, pero que permiten a los interesados, en la UE, hacer un pedido que será distribuido fuera de esta.

La propuesta comentada y graficada por Slaughter y May se cita continuación:

Scenario	Directive applies	GDPR applies
US company without any EU subsidiaries offering free social media services via a website hosted in the US to individuals in the EU	x	✓
Singaporean hotel booking business using cookies to track past customers' (including EU-based customers) browsing in order to target specific hotel adverts to them	x	✓
Chinese flower delivery company allowing data subjects in the EU to make orders for fulfilment only in China	x	✓
Australian retailer with a website for orders/deliveries. The website is accessible to individuals in the EU in English. The currency is the Australian dollar and the address fields only allow Australian addresses	x	x

De esta propuesta se colige que, a entender de Salugther y May, solo quedarían fuera del supuesto de la norma, las empresas que no forman parte de la Unión Europea y que venden bienes o servicios a través de *websites* accesibles en la Unión Europea, pero que, en el campo de las direcciones solo se permiten las del lugar del establecimiento (empresa), la moneda con la que debe pagarse el bien o servicio también es del mismo lugar y el idioma también se circunscribe a la localidad.

Sobre la problemática del carácter extraterritorial del RGPDUE, también se comenta en Wimmer (2018):

> Sin embargo, la aspiración del RGPD a la jurisdicción global no responde a la pregunta de si alguna ley de la UE puede tener un efecto extraterritorial fuera de los límites de Europa. Las reglas y normas de larga data del derecho internacional público deben cumplirse antes de que las agencias reguladoras y los tribunales puedan ejercer su jurisdicción sobre asuntos distantes.[14]

Señala el autor que, si bien el RGPDUE plantea una jurisdicción global, la misma normativa no señala de qué forma una ley de la UE puede tener un efecto extraterritorial fuera de los límites de Europa, salvo las normas conflictuales previstas en cada ordenamiento jurídico, por lo que, en su opinión, debe verificarse, primero, el cumplimiento de las reglas y normas del derecho internacional público y privado, antes de que las agencias reguladoras o los tribunales puedan ejercer jurisdicción sobre asuntos distantes.

En efecto, no existiendo tratados internacionales que generen obligaciones en relación a determinada normativa, parecería imposible que el RGPDUE pueda ser aplicado fuera del territorio de los Estados miembros de la Unión Europea.

3.3.2 A**lcances de la extraterritorialidad del RGPDUE según el TJUE**

Si bien de la lectura del RGPDUE muchos coligieron que este normaba y establecía su propio carácter extraterritorial, con fecha 24 de setiembre de 2019, el Tribunal de Justicia de la Unión Europea ha emitido sentencia en el (Caso C-507/17), con el fin de dilucidar el alcance de la normativa de protección de datos personales de la Unión Europea.

La cuestión planteada en esta sentencia del TJUE del 24 de setiembre del 2019 (CASO 507/17) " consistía en determinar si *Google* se encontraba obligado a proceder con la retirada de la información solicitada en todas las extensiones del dominio de su motor de búsqueda", en razón de la resolución de la Comisión Nacional de Informática y Libertades en su Decisión

[14] Traducción libre al español.

N° 2015-047 de fecha 21 de mayo de 2015 que, determinó que *Google* se encontraba obligado a eliminar de su lista de resultados de búsqueda los datos de una persona.

Conforme cita la sentencia del TJUE del 24 de setiembre del 2019 (CASO 507/17), *Google* se mantuvo firme y se limitó a efectuar un bloqueo o eliminación de los resultados de búsqueda solamente en el espacio territorial de los Estados miembros de la Unión Europea.

Ante ello, la CNIL estimó que Google no había cumplido con el mandato y, mediante Decisión N° 2016-054 del 10 de marzo de 2016, impuso a esta sociedad una sanción de 100 000 euros.

Google solicitó la anulación de la mencionada resolución, mediante demanda presentada ante el *Conseil d'État* (Consejo de Estado actuando como Tribunal Supremo de lo Contencioso-Administrativo, Francia), órgano que planteó una decisión prejudicial ante el Tribunal de Justicia de la Unión Europea.

En virtud de la cuestión prejudicial planteada por el Tribunal Supremo de Francia, es que el TJUE emite la sentencia (CASO 507/17) estimando que:

> "En particular, del tenor de los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 y del artículo 17 del Reglamento 2016/679 no se desprende en modo alguno que el legislador de la Unión haya optado, a fin de garantizar el cumplimiento del objetivo mencionado en el apartado 54 de la presente sentencia, por atribuir a los derechos consagrados en estas disposiciones un alcance que vaya más allá del territorio de los Estados miembros y que haya pretendido imponer a un gestor que, como Google, queda comprendido en el ámbito de aplicación de la Directiva o del Reglamento la obligación de retirar enlaces también de las versiones nacionales de su motor de búsqueda que no correspondan a los Estados miembros." (Fundamento 62)

Con esta decisión, el TJUE ha esclarecido el alcance de la normativa del RGPDUE, estableciendo además un nuevo alcance sobre el denominado "derecho al olvido" que antes había sido estimado por el Tribunal, como un derecho que debía protegerse incluso fuera de las fronteras de la Unión Europea (Véase STJUE C-131/12, Caso Mario Costeja vs Google Spain); limitándolo ahora geográficamente a la Unión Europea.

La aludida sentencia, no sólo enfatiza el alcance del RGPDUE, restringiéndolo a sus Estados miembros, sino que el TJUE reconoce también la importancia de otro derecho fundamental, como el derecho a la libertad de información, señalando que:

STJUE del 24 de setiembre de 2019 (CASO 507/17):

> "Sin embargo, es importante señalar que el interés del público en acceder a una información puede variar, incluso dentro de la Unión, de un Estado miembro a otro, de modo que el resultado de la ponderación que debe llevarse a cabo entre este interés, por un lado, y los derechos al respeto de la vida privada y a la protección de los datos personales del interesado, por otro lado, no será necesariamente el mismo en todos los Estados miembros, máxime cuando, en virtud del artículo 9 de la Directiva 95/46 y del artículo 85 del Reglamento 2016/679, corresponde a los Estados miembros establecer, en particular para los tratamientos realizados exclusivamente con fines periodísticos o con fines de expresión artística o literaria, las exenciones y excepciones necesarias para conciliar esos derechos con, entre otras cosas, la libertad de información." (Fundamento 67)

En efecto, el TJUE ha reconocido que, si bien el derecho a la protección de datos es un derecho fundamental de especial relevancia por su vinculación con la vida privada y con la autonomía del individuo, este no es un derecho absoluto, por lo que, en la ponderación con otros derechos, como el derecho a la información debe efectuarse un particular análisis a la luz del interés público que pudiere subyacer a la revelación de la información.

Como bien señala el Tribunal, el equilibro de los derechos en juego puede variar en los países alrededor del mundo e incluso dentro de la propia Unión Europea. Resultando apropiado que la justicia europea haya reconocido la soberanía de cada Estado, la diferencia de enfoques y por ende la diferencia de las legislaciones que corresponde a cada sistema en particular.

3.3.3 **Desafíos económicos de la Protección de Datos Personales**

En un comunicado de prensa del 27 de enero de 2017, la consultora *Price Water House Cooper* reveló una encuesta realizada a compañías de EE. UU. en relación con la implementación de las reglas establecidas en el RGPD (hasta ese momento publicado, pero aún no vigente). El resultado arrojó lo siguiente:

PwC (2017):

> Nueva York, 23 de enero de 2017. En una encuesta reciente, casi todos los encuestados (92 %) consideraron el cumplimiento del histórico Reglamento General de Protección de Datos (RGPD) de Europa como una prioridad en su agenda de seguridad y seguridad de datos en 2017, más de la mitad de los encuestados dice que es "a" prioridad principal y el 38 % dice que está "entre" las principales prioridades. La Encuesta de Pulso de Preparación de RGPD publicada hoy por *PwC US* examina la preparación de RGPD en los EE. UU. ¿Y por qué las compañías estadounidenses están dispuestas a gastar $ 1 millón o más en planes de preparación de RGPD? […]
>
> "Las multinacionales estadounidenses que no han tomado medidas significativas para prepararse para RGPD ya están detrás de sus pares", dijo Jay Cline, líder de privacidad de *PwC* en Estados Unidos, señalando, además, que "cuando los reguladores europeos de 2017 clarifiquen aun más cómo interpretan RGPD, es probable que más empresas estadounidenses vuelvan a evaluar el retorno de la inversión de sus iniciativas europeas". (p. 1)

De otro lado, Brandon (2018) señala:

> No todo el mundo está listo para el RGPD, pero las empresas de *Google* han estado actualizando silenciosamente sus términos, reescribiendo contratos y desplegando nuevas herramientas de datos personales en preparación para el cambio masivo en el panorama legal. Hasta ahora, ha sido un gran problema para los departamentos legales, pero a medida que los cambios de política y las peleas contractuales se hacen públicos, también ha comenzado a afectar al usuario medio de la web. (p. 1)

A nivel jurisprudencial ya se había establecido el carácter extraterritorial de las normas de protección de datos, analizándose la Directiva 95/46 de Protección de Datos Personales. Por ejemplo, en la Sentencia del caso Costeja vs *Google Spain* emitida por el TJUE, donde se señaló:

> 46. […] la actividad de promoción y venta de espacios publicitarios, de la que *Google Spain* es responsable para España, constituye la parte esencial de la actividad comercial del grupo *Google* y puede considerarse que está estrechamente vinculada a *Google Search*.
>
> 54. En este marco, cabe señalar que se desprende, concretamente de los considerandos 18 a 20 y del artículo 4.° de la **Directiva 95/46**, que el legislador de la Unión pretendió evitar que una persona se viera excluida de la protección garantizada por ella y que se eludiera esta protección, estableciendo un ámbito de aplicación territorial particularmente extenso.

Así, en las conclusiones de la referida sentencia, el Tribunal de Justicia de la Unión Europea señaló:

> […]

> 2) El artículo 4.°, apartado 1, letra "a" de la Directiva 95/46 debe interpretarse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.

En dicho contexto, en atención a los anteriores pronunciamientos del TJUE, algunas de las empresas de tecnología en EE. UU. ya venían implementando las medidas ahora establecidas legislativamente en el RGPDUE.

De otro lado, encontrándose publicado el RGPDUE, pero no vigente a la fecha, en referencia de la siguiente cita, *Facebook* venía introduciendo nuevos controles de privacidad. Según Thuy Ong (2018):

> *Facebook* está introduciendo nuevos controles de privacidad para cada uno de sus 2000 millones de usuarios como parte del cumplimiento del Reglamento General de Protección de Datos de la UE (RGPD) que entrará en vigencia el 25 de mayo. *Facebook* pedirá a los usuarios, independientemente de dónde vivan, que revisen sus opciones de privacidad, desde la información que agreguen a su perfil hasta cómo *Facebook* usa sus datos para orientar los anuncios. (…) **El CEO *Mark Zuckerberg* indicó que *Facebook* extendería sus controles de protección de datos europeos a nivel mundial**. […] Los usuarios europeos también verán los detalles de contacto del Oficial de Protección de Datos de *Facebook*, que es un requisito bajo RGPD. (p. 1)

Estos mismos argumentos volvieron a ser expuestos por el CEO de *Facebook* el 22 *de* mayo de 2018 ante los cuestionamientos de los senadores del Parlamento Europeo, según se

recogió en la prensa chilena.[15] Por su parte, *Twitter*, conforme comentó su vicepresidente,[16] ha tenido avances en cuanto a la implementación de la nueva regulación europea establecida en el RGPDUE.

De otro lado, *Apple*, *Microsoft* y *Google Cloud* llevan la ventaja en temas de seguridad, ya que vienen alineándose a la nueva normativa según información en sus portales web.

Sin embargo, y dada la incertidumbre inicial, a la entrada en vigencia del RGPDUE, algunos medios de comunicación establecidos en los EE. UU. decidieron restringir el acceso a sus páginas web a los países europeos.[17]

De esta manera, se advierte la afectación comercial de los medios de comunicación situados fuera de Europa y que, ante la falta de implementación de la regulación establecida en el RGPDUE, o ante la incertidumbre de su correcta aplicación, al momento de la entrada en vigencia de esta normativa, 25 de mayo de 2018, decidieron restringir el acceso de sus contenidos al territorio de la Unión Europea.

[15] BioBio, Chile (2018):

Zuckerberg: *"*Actualmente, existen miles de personas trabajando para implementar las disposiciones del RGPD, no obstante, menciona que esto debe estar abierto al debate para no perjudicar el avance de la tecnología. Asimismo, ha efectuado un *mea culpa*, y afirmó que la seguridad no puede garantizarse al 100 %, pues siempre se crean nuevas tecnologías que pueden afectar la misma, pero que con los ajustes de seguridad que se vienen implementando desde el 2014 se encuentran en una mejor posición".(p.1)

[16] Diario Gestión (2018):

Crowell: La red social "pone todo el esfuerzo" en desarrollar herramientas de inteligencia artificial contra los "*bots*" o cuentas fantasmas pensadas para manipular y extender las llamadas "*fake news*" o noticias falsas. "Hemos invertido mucho en inteligencia artificial para buscar señales y comportamiento en cuentas que nos pongan sobre la pista. Se trata de analizar comportamientos y otras pistas, pero nunca contenido u origen".

Señaló que hay "diferencias fundamentales" entre plataformas. *Twitter* es diferente (de *Facebook* o *Instagram*) principalmente porque en nuestro caso todo es público y abierto desde el principio, no almacenamos información privada, nuestros productos de datos son directamente en abierto", explicó.

"Hemos trabajado desde hace mucho tiempo para ponernos al día con el RGPD, que creemos que es lo más beneficioso para todos, porque permite que la gente entienda cuáles son los derechos e implicaciones", dijo Crowell, quien añadió que se ha creado la figura de un oficial de protección de datos no solo para la Unión Europea, sino para todo el mundo (p. 1).

[17] Al respecto, Rodella (2018), en su artículo periodístico, nos indica lo siguiente:

"Si usted se encuentra en la Unión Europea y quiere mantenerse informado sobre qué pasa en Estados Unidos con las noticias de *Los Angeles Times*, le espera una mala sorpresa. Desde el pasado viernes, día de la entrada en vigor del nuevo Reglamento General de Protección de Datos (RGPD), las páginas web de este y otras decenas de medios estadounidenses tienen el acceso restringido para los usuarios que se conectan desde la UE. Entre los diarios a cuyas webs no se puede acceder están *Chicago Tribune*, *New York Daily News* y *The Baltimore Sun*, de propiedad tal y como el periódico californiano de la compañía *Tronc*. También *Lee Enterprises*, otra empresa que gestiona distintos medios de comunicación de EE. UU., deniega el acceso a sus páginas web para los lectores que intentan acceder desde Europa." (p.1)

Se ha considerado pertinente citar estas notas periodísticas a efectos de capturar el momento y la incertidumbre que aconteció en diversos medios y compañías estadounidenses en el periodo inicial de la entrada en vigencia del RGPDUE.

Pero, ¿cuáles son los reales objetivos que se deben tener en cuenta con la finalidad de dotar de seguridad y fluidez al comercio entre EE. UU. y Europa? Podemos mencionar que uno de los esfuerzos en este ámbito se dio con la Decisión 2000/520/CE[18], de fecha 26 de julio del 2000.

De acuerdo con lo comentado por Lombarte (2017):

> Mediante la Decisión 2000/520/CE, la Comisión Europea reconoció un *sui generis* nivel de protección adecuado de los datos personales en EEUU llamado «régimen de puerto seguro» (*Safe Harbour*) consistente en proclamar una serie de principios de protección de datos personales a los que las empresas estadounidenses podían suscribirse voluntariamente. (p.605).

Sin embargo, en razón de la denuncia interpuesta por un usuario de Facebook el Sr. Schrems, basaba en que los datos personales de los usuarios de la red social Facebook ubicados en la Unión Europea, se trasladaban sin ningún tipo de control y/o seguridad a los servidores instalados en Estados Unidos y que estos no contaban con la protección tecnológica necesaria para salvaguardar la confidencialidad del caso, la Decisión 2000/520/CE fue declarada inválida por el TJUE – Gran Sala en el asunto 362-/14 de fecha 06 de octubre de 2015.

El TJUE discrepó de los argumentos de la Sala Irlandesa que, había señalado que, la transferencia de los datos de los ciudadanos de la Unión Europea a servidores ubicados en Estados Unidos contaba con todos los estándares suficientes para la protección de datos personales que eran trasferidos.

[18] La Decisión 2000/520/CE regula los principios de puerto seguro (*Safe Harbour*) que garantizan un nivel de protección adecuado de los datos personales transferidos por las compañías europeas a empresas de Estados Unidos adheridas a dichos principios.

El TJUE analizó la diferencia de tratamiento en la protección de los datos personales que otorga Estados Unidos, conforme a los fundamentos de la sentencia del 06 de octubre del 2015 C-306/14, reseñados por Lombarte (2018):

> a) "No se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización" (punto 93).
>
> b) "En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7.° de la Carta" (punto 94).
>
> c) "Una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47.° de la Carta… La existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho" (punto 95). (pp. 608-609)

Posteriormente, con fecha 12 de julio de 2016, la Comisión Europea adoptó el acuerdo denominado *Privacy-Shield* o Escudo de Privacidad, consistente en un sistema de autocertificación por parte de compañías de los EE. UU.

La Decisión 2013/1250 de la Comisión Europea, mediante la cual se adopta el Escudo de Privacidad, indica en su apartado 2(15) que:

> "Sin perjuicio del cumplimiento de las disposiciones nacionales adoptadas en aplicación de la Directiva 95/46/CE, la presente Decisión tiene por efecto que se autoricen las transferencias de un responsable o encargado del tratamiento en la Unión a organizaciones de los Estados Unidos que hayan autocertificado su adhesión a los principios con el Departamento de Comercio y se hayan comprometido a atenerse a ellos. Los principios se aplican únicamente al tratamiento de datos personales realizado por la organización de los EE. UU. siempre que el tratamiento por dichas organizaciones no entre en el ámbito de aplicación de la legislación de la Unión. El Escudo de la privacidad no afecta a la aplicación de la legislación de la Unión que regula el tratamiento de los datos personales en los Estados miembros."

Este mecanismo de autocertificación previsto por el *Privacy-Shield* o Escudo de Privacidad no ha estado exento de críticas, así a decir de Bu-Pasha (2017):

> Algunos principios del Escudo de Privacidad ya han sido criticados, como la provisión de "autocertificación", la posición del Defensor del Pueblo con dudosa independencia (...). Se argum2enta que el lenguaje y la disposición del Escudo de Privacidad son un poco ambiguos, inconsistentes, poco claros y difíciles de entender en algunos aspectos. Debido a que muchos términos se interpretan de manera diferente en la UE y en los Estados Unidos, y algunas terminologías son diferentes, pero significan lo mismo en esos dos territorios, es muy importante explicar cada término confuso con definiciones claras. (p. 225)

Las críticas al *Privacy Shield* cobraron aún mayor importancia en virtud del caso *Facebook* y *Cambridge Analytica*, ambas empresas registradas dentro del marco de este acuerdo.

El *Privacy Shield* ha sido declarado inválido recientemente por el TJUE, en la sentencia emitida el 16 de julio de 2020, recaída en el Caso C-311/2018, a raíz del reclamo del señor Maximillian Schrems contra Facebook Ireland Ltd, donde el citado ciudadano austriaco cuestionó la seguridad del tratamiento de sus datos por parte de Facebook Inc. en los Estados Unidos, datos a los que esta compañía accedía a través de su filial en la Unión Europea, en tanto Facebook se encontraba certificada mediante el sistema del *Privacy Shield*.

Es así que, en la sentencia recaída en el Caso C-311/2018, el Tribunal ha considerado que "a no ser que exista una decisión de adecuación válidamente adoptada por la Comisión, la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión" (Fundamento 121)

Para el TJUE, el gobierno de EE.UU. podría justificar el acceso y utilización de datos personales de ciudadanos de la Unión Europea sobre la base de su propia legislación y sobre la base de principios como la seguridad nacional e interés público. Por tanto, las transferencias de datos desde la Unión Europea hacia EE.UU. no se encontrarían debidamente protegidas de acuerdo a la normativa prevista en el RGPDUE.

Asimismo, para el TJUE la justicia americana tampoco garantizaría a los ciudadanos europeos el derecho a la tutela jurisdiccional efectiva, en tanto, la figura del Defensor del Pueblo prevista en el Privacy Shield no permite acceder a los mismos recursos que prevé la justicia estadounidense ordinaria e incluso las normas sobre seguridad de Estado excluyen cualquier tipo de recurso.

Capítulo IV

Protección de Datos Personales en el Perú

En el Perú, el derecho a la Protección de Datos Personales se encuentra positivizado en la Ley 29733, que data del año 2011, en adelante "la Ley", que prevé como su objeto principal garantizar el derecho fundamental a la protección de los datos personales.

4.1. Del objeto del derecho de protección de datos personales según la legislación peruana

La Ley 29733 señala como objeto de protección de datos personales, al derecho fundamental preceptuado de esta manera en el artículo 2.° numeral 6, de la Constitución Política del Perú:

> Artículo 2.- Toda persona tiene derecho:
>
> (…)
>
> 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Sin embargo, a entender de León (2011), el derecho previsto en el artículo 2°, numeral 6. de la Constitución no se corresponde con el derecho a la autodeterminación informativa, en la forma en que este ha sido concebido y desarrollado en Europa, en tanto, para el autor, la protección que otorga el Estado peruano se encontraría estrechamente vinculada y limitada al derecho a la intimidad de la vida privada y familiar mas no al derecho a la protección de datos personales, en donde el objeto de protección es el individuo en sí mismo (p.92).

El Tribunal Constitucional peruano, no obstante, mediante STC 00146-2015-PHD/TC, ha señalado que, el inciso 6 del artículo 2 de la Carta Magna si consagra el derecho de

autodeterminación informativa que, como se comenta en Puldain (2018 : 125) es el derecho que subyace al derecho a la protección de datos personales.

Se encuentre o no previsto el derecho a la autodeterminación informativa en la Ley o en la Constitución, este derecho, ha sido materia de desarrollo jurisprudencial por parte del Tribunal Constitucional, conforme con lo siguiente:

> "El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. Se encuentra estrechamente ligado a un control sobre la información, como una autodeterminación de la vida íntima, de la esfera personal.
>
> Mediante la autodeterminación informativa se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos; por tanto, no puede identificarse con el derecho a la intimidad, personal o familiar, ya que mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen" (STC 04729-2001-PDH/TC, Fundamento 4.)

De esta manera, desde la jurisprudencia del Tribunal Constitucional se ha dotado de contenido al derecho objeto de protección de la Ley peruana sobre Protección de Datos Personales.

En relación con la regulación prevista en el Reglamento de la Ley de Protección de Datos, aprobado mediante Decreto Supremo N° 03-2013-JUS, en adelante "el Reglamento", nos comenta León (2013) que, la definición de datos personales en el Reglamento, "parece un dictado adecuado, más bien, a los intereses de quienes tratan datos personales y, no de los titulares de la autodeterminación informativa" (p. 16).

La precitada definición de los datos personales, como toda información sobre una persona natural que la identifica, o la hace identificable, a través de medios que pueden ser razonablemente utilizados; permitiría que se excluya a aquella información que permita la identificación del individuo de manera indirecta y además se mantiene la ambigüedad de la Ley, en relación a lo que pudiera entenderse por *razonable*.

Para el citado autor, además, la Ley 29733 – Ley de Protección de Datos Personales establece excepciones que no se encuentran debidamente justificadas, señalando como ejemplo la primera excepción prevista en el artículo 15.° de la Ley 29733:

> **Artículo 15. Flujo transfronterizo de datos personales**
>
> El titular y el encargado de tratamiento de datos personales deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley.
>
> En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto por la presente Ley.
>
> No se aplica lo dispuesto en el segundo párrafo en los siguientes casos:
>
> 1. Acuerdos en el marco de tratados internacionales sobre la materia en los cuales la República del Perú sea parte.

Esta excepción en la ley peruana resulta menos estricta, si la comparamos con la exigencia de la Unión Europea, donde se requiere de sistemas de certificación que cumplan con estándares adecuados para la transferencia de datos de ciudadanos de la Unión Europea hacia empresas de los EE. UU.

4.2. Del "alcance extraterritorial" de la normativa peruana sobre protección de datos personales según la autoridad nacional

Mediante Resolución Directoral N° 026-2016-JUS/DGPDP, de fecha 11 de marzo de 2016, la Dirección General de Protección de Datos Personales (Autoridad Nacional de Protección de Datos Personales creada mediante Ley 29733) declaró infundado el recurso de reconsideración planteado por *Google* contra la Resolución Directoral N° 045-2015-JUS/DGPDP, de fecha 30 de diciembre de 2015, confirmando la misma que, resolvió "ordenar a *Google* bloquear los datos (nombre y apellido) que aparecen en los resultados del motor de búsqueda Google Search". (Art. 2°)

El caso trataba sobre el reclamo de un ciudadano peruano que había solicitado a Google el bloqueo o eliminación de los resultados que resultaban de la búsqueda de su nombre relacionados con una causa penal sobreseída.

La autoridad nacional acogió el pedido del reclamante, considerando que, el derecho de protección datos de un ciudadano peruano debe hacerse valer no sólo en el Perú sino en cualquier parte del mundo, indicando en la R.D. N°026-2016-JUS/DGPDP que, "la hipervisibilización de información personal de ciudadanos peruanos sin consentimiento, no solo vulnera el derecho fundamental a la protección de datos personales del reclamante en el Perú sino a nivel planetario". (Fundamento 5.3.3.)

En la mencionada R.D. N° 026-2016-JUS/DGPDP, la autoridad nacional consideró que el derecho de protección de datos personales por ser un "derecho fundamental" debe protegerse incluso más allá de nuestras fronteras refiriendo que:

> De otro lado, debe tenerse claro que lo que determina que los resultados de búsqueda que aparecen en el motor de búsqueda Google Search estén dirigidos a usuarios localizados en el Perú, no es la ubicación física de quien indaga la información, sino el criterio por el cual se

busca tal información, y ese criterio de búsqueda (como se ha explicado en la resolución impugnada) corresponde a una búsqueda nominal: "los nombres y los apellidos" del reclamante. En consecuencia, esta autoridad considera que, al ser el reclamante un ciudadano peruano que radica en el Perú y siendo innegable que sus datos son tratados por el buscador y puestos a disposición de quienes buscan información sobre su persona, *estén ubicados en territorio nacional o no, es decir, desde donde sea y a donde sea, dicho ciudadano peruano es titular del derecho a la protección de datos personales*, y la vigencia real de tal derecho ser debe ser exigida a quien lo afecte. (p.26)

Si bien la Dirección General de Protección de Datos señala que, para la resolución de este caso, la STJUE del 13 de mayo de 2014 (Caso Google Spain) sólo se ha tenido como referencia y no ha sido el factor determinante de su decisión, resulta evidente que, de las R.D. 026-2016-JUS/DGPDP y R.D. N° 015-2015-JUS/DGPDP no se advierte un análisis detallado del ámbito de aplicación territorial de la normativa según lo previsto en el artículo 5° del Reglamento[19], otorgándole al derecho de autodeterminación informativa del ciudadano peruano reclamante, una protección de alcance global.

[19] **Decreto Supremo N° 003-2013-JUS Reglamento de la Ley de Protección de Datos Personales**

Artículo 5.- Ámbito de aplicación territorial.

Las disposiciones de la Ley y del presente reglamento son de aplicación al tratamiento de datos personales cuando:

1. Sea efectuado en un establecimiento ubicado en territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento.

2. Sea efectuado por un encargado del tratamiento, con independencia de su ubicación, a nombre de un titular de banco de datos personales establecido en territorio peruano o de quien sea el responsable del tratamiento.

3. El titular del banco de datos personales o quien resulte responsable del tratamiento no esté establecido en territorio peruano, pero le resulte aplicable la legislación peruana, por disposición contractual o del derecho internacional; y

4. El titular del banco de datos personales o quien resulte responsable no esté establecido en territorio peruano, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento.

Para estos efectos, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que imponen la Ley y el presente reglamento y designará un representante o implementar los mecanismos

Sin embargo, surge la siguiente cuestión: ¿será que, a la luz de la actual jurisprudencia del Tribunal de Justicia de la Unión Europea, en el comentado Caso C-507/17 (Google - CNIL Francia), nuestra Autoridad Nacional de Protección de Datos Personales cambiará de opinión?

suficientes para estar en posibilidades de cumplir de manera efectiva, en territorio peruano, con las obligaciones que impone la legislación peruana.

Cuando el titular del banco de datos personales o quien resulte el responsable del tratamiento no se encuentre establecido en territorio peruano, pero el encargado del tratamiento lo esté, a este último le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el presente reglamento.

En el caso de personas naturales, el establecimiento se entenderá como el local en donde se encuentre el principal asiento de sus negocios, o el que utilicen para el desempeño de sus actividades o su domicilio.

Tratándose de personas jurídicas, se entenderá como el establecimiento el local en el que se encuentre la administración principal del negocio. Si se trata de personas jurídicas residentes en el extranjero, se entenderá que es el local en el que se encuentre la administración principal del negocio en territorio peruano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad.

Si no fuera posible establecer la dirección del domicilio o del establecimiento, se le considerará con domicilio desconocido en territorio peruano.

CONCLUSIONES

Como se ha referido en el presente trabajo, algunos sectores critican la emisión unilateral de normas que establecen por sí mismas su alcance extraterritorial (aplicación de la legislación comunitaria de la UE a otros países), pues lo consideran un ataque al desarrollo de las normas internacionales y al derecho internacional. No obstante, la emisión de normas con carácter extraterritorial, surgen de la pretensión de los Estados de hacer valer los derechos de sus ciudadanos incluso fuera de sus fronteras y en este contexto también ha surgido el denominado principio de jurisdicción universal.

Las empresas de tecnología, por la forma en que presentan sus servicios, así como aquellas que utilizan el ciberespacio para ofertar bienes y servicios**,** se encontrarían, ante la disyuntiva sobre el cumplimiento o no de la legislación establecida para la Unión Europea, tal vez no por la "extraterritorialidad" en sí de la normativa europea, ni por el *enforcement* que implicaría que sus autoridades les hagan cumplir las sentencias extranjeras, pero sí por otros factores como el prestigio y la salvaguarda de sus propios intereses en el comercio con Europa.

En el comentado Debate sobre Privacidad y Seguridad en la Red: Regulación en los Mercados, también fue materia de discusión el posible estancamiento del dinamismo comercial, la innovación y el desarrollo de nuevos negocios frente a un marco muy estricto para la protección de los datos personales de los individuos que se establece en el RGPDUE.

Si bien el RGPDUE carece de obligatoriedad en los demás Estados soberanos, este es un instrumento que, intenta atenuar las consecuencias del comercio, en un mundo globalizado, y su incidencia en la esfera personalísima de sus ciudadanos. En este sentido, la valoración del derecho a la protección de datos personales en la Unión Europea prevalece a los fines económicos en contratar con empresas de todas partes del mundo.

Contrariamente a la considerable valoración del derecho de protección de datos personales por parte de la Unión Europea, las empresas americanas, lo que persiguen es un interés económico, siendo que, muchas de ellas mantienen activos, vínculos comerciales y crecientes expectativas en los nuevos negocios que puedan desarrollar con los países de la Unión Europea.

La dicotomía de enfoques en materia de protección de datos personales, conforme hemos comentado, difiere en sustancia, entre la Unión Europea y EE.UU., situación que preocupa, en tanto a la fecha los acuerdos de *Safe Harbour* y *Privacy Shield* que permitían un mayor dinamismo en el comercio entre la Unión Europea y los Estados Unidos de América, han sido invalidados por el Tribunal de Justicia de la Unión Europea.

Por el momento, se prevé que, será un motivo "económico" y de "reputación" más que de índole legal obligatorio, el que determine, en el análisis particular de cada empresa la conveniencia de adecuar sus estándares de protección a lo señalado por la norma europea.

Finalmente, en lo que respecta a nuestro país, al igual que en la Unión Europea, se ha reconocido el derecho a la protección de datos como un derecho fundamental, sin embargo, dada la asimetría de poderes frente a un país como EE.UU. y nuestro interés en incrementar el comercio con ese país, resultaría idóneo, implementar mecanismos que permitan un flujo transfronterizo de datos que respete los estándares mínimos de seguridad; y en el ámbito de su alcance territorial determinar sanciones que cumplan un real rol disuasivo.

REFERENCIAS

- Agencia Española de Protección de Datos. (2017). *Guía del Reglamento General de Protección de Datos*. Madrid. Recuperado de: https://libros-revistas-derecho.vlex.es/source/publicaciones-agencia-espa-ola-proteccion-datos-21826
- Alfu, U. (2018). *Extraterritorialidad del Reglamento General de Protección de Datos de la Unión Europea-GCC Views*. Gccviews.com. Recuperado de: https://gccviews.com/extraterritorialidad-del-reglamento-general-de-proteccion-de-datos-de-la-union-europea
- BBC News Mundo. (2020). *Qué es el Brexit y otras 5 preguntas básicas para entender la salida de Reino Unido de la Unión Europea*. Recuperado de: https://www.bbc.com/mundo/noticias-internacional-46521624
- BioBio Chile. (25 de mayo de 2018). *Mark Zuckerberg responde ante el Parlamento Europeo por la filtración de datos de Facebook.* Recuperado de: https://www.youtube.com/watch?v=f966kRxGkko
- Bossio, Jorge. (2008). *Privacidad de datos: los límites de Internet y el acceso a la información.* Lima: Palestra, Portal de Asuntos Públicos de la PUCP. Recuperado de: http://palestra.pucp.edu.pe/?id=393
- Brandon, R. (2018). *GDPR launches today. Here's what you need to know. The Verge* Recuperado de: https://www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice
- Broseta, Manuel. (2005). *Manual de Derecho Mercantil.* 12.ª edición, Vol. 1 p. 55. Fernando Martinez Sanz (ed.). Madrid: Editorial Tecnos.

- Bu-Pasha, Shakila. (2017). *Cross-border issues under EU data protection law with regards to personal data protection, Information & Communications Technology Law*, 26:3, 213-228, doi: 10.1080/13600834.2017.1330740.
- Calderón, A. (2010). *Balotario desarrollado para el examen de CNM.* Lima: Editorial San Marcos.
- Caso n.° 19-cv-2184. (24.07.2019). EE. UU. vs *Facebook Inc*. Orden dispuesta por la Corte del Distrito de Columbia de los Estados Unidos de América. Sanción civil, sentencia monetaria y medidas cautelares.
- Chanamé, R. (2014). *Diccionario jurídico moderno.* Lima: Lex y Iuris.
- Chiovenda, G. (1954). *Instituciones del derecho procesal civil*. Madrid: Editorial Revista de Derecho Privado.
- Comisión Europea. (2016). "Reforma de la Protección de Datos en Europa. Ventajas para las empresas de la Unión Europea". En *Ficha Informativa de la Dirección Nacional de Justicia y Consumidores de la Unión Europea*. Recuperado de: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41593
- Decisión N°2015-047 del 21 de enero de 2015. Comisión Nacional de Informática y Libertades de Francia, CNIL vs. GOOGLE LLC. Recuperado de: https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000030746525
- Delgado, C., Delgado M y Lincoln, C. (2002). *Introducción al derecho internacional privado* (pp. 43 y ss.) Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú.
- Deliberación N°2016-054 del 10 de marzo de 2016. Comisión Nacional de Informática y Libertades de Francia, CNIL vs. GOOGLE LLC. Recuperado de: https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946

- Deliberación SAN-2019-001 del 21 de enero de 2019. Comisión Nacional de Informática y Libertades de Francia, CNIL vs. GOOGLE LLC. Recuperado de: https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1
- Departamento de Comercio de los Estados Unidos de America (2020). Privacy-Shield. Recuperado de https://www.privacyshield.gov/program-overview
- Colin Crowell. (2018). "Trabajamos duro contra los bots y las fake news". *Gestión*, junio de 2018. Recuperado de: https://gestion.pe/tecnologia/vicepresidente-twitter-duro-bots-fake-news-234953-noticias
- De Llano, P. (2018). "Una consultora que trabajó para Trump manipuló datos de 50 millones de usuarios de Facebook". *El País*. Recuperado de: https://elpais.com/internacional/2018/03/17/estados_unidos/1521308795755101.html
- Espinosa, G. (2018). *GDPR: Lo que debes saber sobre el reglamento europeo de protección de datos personales*. Recuperado de: https://solcargo.mx/gdpr-lo-que-debes-saber-sobre-el-reglamento-euopeo-de-proteccion-de-datos-personales
- Ewing, Mike, "The Perfect Storm: The Safe Harbour and the Directive on Data Protection", en "Houston Journal of International Law", vol. 24, 2002, p. 315 y s.
- Expansión (2018). *Guía práctica: GDPR*. Recuperado de: https://www.expansion.com/especiales/2018/GDPR/
- Fair, Lesley. (2019). *Lo que significa el acuerdo de la FTC con Facebook para consumidores*. Blog FTC. Recuperado de: https://www.consumidor.ftc.gov/blog/2019/07/lo-que-significa-el-acuerdo-de-la-ftc-con-facebook-para-consumidores.
- Fernández, R. J. C., y L. S. Sánchez. (2013). *Derecho internacional privado* (p. 53). Cizur Menor. Navarra: Civitas-Thomson Reuters.

- Fundación Telefónica. (2012). *El debate sobre la privacidad y seguridad en la red: regulación y mercados* (p. 44). Madrid: Fundación Telefónica.
- Gacitua, A. (2014). *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea.* Recuperado de: https://ddd.uab.cat/pub/tesis/2014/hdl_10803_284352/alge1de1.pdf
- González, A. Roberto. (2014): "El nuevo paradigma de la garantía de la jurisdicción", *Ars Boni Et Aequi* (año 10, n.° 1, pp. 119-150).
- Gonzáles, S. (2016). *La protección de datos de carácter personal en la gestión de los recursos humanos de la empresa*. Recuperado de: https://rio.upo.es/xmlui/bitstream/handle/10433/3054/garcia-coca-tesis16.pdf?sequence=1&isAllowed=y
- Gutiérrez, A. (2012). *Nuevas tecnologías, protección de datos personales y proceso penal*. Madrid: La Ley.
- Guzmán, M. (2013). *El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español*. Recuperado de: http://eprints.ucm.es/22817/1/T34727.pdf
- Hernández, Z. J. (2010). "Las empresas transnacionales y los derechos humanos: El control social y normativo de las empresas transnacionales". *Foro Jurídico*, 11, p. 272 y ss.). PUCP.
- Herrera, L. (1960). *Derecho internacional privado y tema conexos.* Caracas: El cojo S. A.
- Kacowicz, Arie y Mor Mitrani. (2016). "Por qué no tenemos teorías coherentes sobre la globalización". En *Foro Internacional* (vol. 56 n.° 2, abr/jun). México. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-013X2016000200378

- Koskenniemi, Martti. (2010). "El Destino del Derecho Internacional Público: Entre la técnica y la política". En *Revista de Derecho Público de Facultad de Derecho de la Universidad de Los Andes*, n.° 24, marzo. Recuperado de: https://derechopublico.uniandes.edu.co/components/com_revista/archivos/derechopub/pub86.pdf
- Kozlowska y Timmons. (2018). *What We Learned from Mark Zuckerberg's Congressional Testimony.* Quartz. Recuperado de: https://qz.com/1251646/what-we-learned-from-mark-zuckerbergs-congressional-testimony
- León, Leysser. (2011). "Manipulación de información personal y derechos fundamentales. Crítica del proyecto de «Ley de protección de datos personales»". *Actualidad Jurídica, N° 210, Lima, p. 91 y s*.
- León, Leysser. (2013). "Malas leyes, peores reglamentos. Apuntes críticos sobre el porvenir de la tutela de la persona frente al tratamiento de datos en el Perú". *Revista Actualidad Jurídica, Abril. N° 233, Lima, p.13 y ss*. Recuperado de: https://works.bepress.com/leysser_leon/19/
- Lombarte, Artemi. (2017). *"El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet". Teoría y realidad constitucional,* n.° 39. Madrid: UNED.
- Martínez-Martínez, Dolores-Fuensanta. (2018). "Unification of Personal Data Protection in the European Union: Challenges and Implications". *El profesional de la información.* (Vol. 27, n.° 1, pp. 185-194). Recuperado de: http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17_esp.pdf
- Meján, L. C. (1996). *El derecho a la intimidad y la informática.* México D. F.: Porrúa.
- Monroy, Gerardo. (1995). *Tratado de derecho internacional privado*. Bogotá, Colombia: Temis (pp. 65 y ss).

- Moya, P. (2010). *El derecho a ser informado como sustento fundamental del control de datos personales*. Recuperado de: http://repositorio.uchile.cl/tesis/uchile/2010/de-moya_p/pdfAmont/de-moya_p.pdf
- Munizlaw.com. (2018). *Alerta, comunicaciones y privacidad.* Recuperado de: http://www.munizlaw.com/Productos/alerta-legal/Comunicaciones/2018/alerta%20telecom-1-2018.htm
- Newsroom.fb.com. (2018). "An Update on Our Plans to Restrict Data Access on Facebook", *Facebook Newsroom*. Recuperado de: https://newsroom.fb.com/news/2018/04/restricting-data-access
- Organización de los Estados Americanos-Secretaría de Asunto Jurídicos. (2012). *Estudio comparativo: protección de datos en las Américas*. Whashington D. C. Recuperado de: http://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12.pdf
- Ornelas Nuñez, y M. Higuera Pérez. (2013). "La autorregulación en materia de protección de datos personales: la vía hacia una protección global". En *Revista de Derecho, comunicaciones y nuevas tecnologías*. Universidad de Los Andes, Facultad de Derecho, n.° 9. Junio. Recuperado de: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics130.pdf
- Orrego, César. (2013). Una Aproximación al Contenido Constitucional del Derecho de Autodeterminación Informativa. Anuario de Derecho Constitucional Latinoamericano, año XIX, pp. 311-330. Bogotá. Recuperado de: http://www.corteidh.or.cr/tablas/r32202.pdf
- Ortega, Alfonso. (2007). "Transferencia internacional de datos de carácter personal: UE vs. EE. UU.". En *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elchi* (Vol. I, n.° 2, marzo. pp. 210-219).

- Ossorio, M. (2014). *Diccionario de Ciencias Jurídicas Políticas y Sociales*. Guatemala: Datascan S.A.
- Parrish, Austen L. (2008). *Reclaiming International Law from Extraterritoriality* (25 de febrero). Universidad de Indiana. Recuperado de: https://ssrn.com/abstract=1013740 or http://dx.doi.org/10.2139/ssrn.1013740
- Parrish, Austen. (2017). "The Interplay Between Extraterritoriality, Sovereignty, and the Foundations of International Law" (24 de marzo), cap. 12. En *Standards and Sovereigns: Legal Histories of Extraterritoriality, Forthcoming*. Recuperado de: SSRN: https://ssrn.com/abstract=2940361
- Parrish, Austen L. (2017). "Fading Extraterritoriality and Isolationism? Developments in the United States", *Indiana Journal of Global Legal Studies* (Vol. 24: Iss. 1, Article 9). Recuperado de: https://www.repository.law.indiana.edu/ijgls/vol24/iss1/9
- Peltz-Steele, Richard J. (2015). *The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation* (n.° I, vol. 19, julio de 2015). Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2637010
- Pérez, Juan Pablo. y Patrick Wieland. (2007). "La actuación extraterritorial del Estado: re-examinando el ámbito *ratione loci* desde el Derecho internacional contemporáneo". *Revista Lus et Vertias*. (17) (34). pp. 277-291.
- Poschl, Magdalena. (2015). "La garantía de los estándares de Derechos Humanos y fundamentales ante las nuevas amenazas que generan los particulares y los actores extranjeros". En *Revista Teoría y Realidad Constitucional*, n.° 36, 2015. UNED. Recuperado de: http://revistas.uned.es/index.php/TRC/article/view/16072

- Puldain Salvador, V. (2018). “El futuro marco legal para la protección del acceso a los datos”. *Revista Ibero-Latinoamericana de Seguros (Vol. 26, Issue 47, pp. 119-135).* Recuperado de: https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/21178
- PwC. (2017). *GDPR Compliance Top Data Protection Priority for 92 % of US Organizations in 2017, According to PwC Survey.* Recuperado de: https://www.pwc.com/us/en/press-releases/2017/pwc-gdpr-compliance-press-release.html
- Rodella, Francesco. (2018). “La nueva norma de protección de datos pone a prueba a la administración y empresas”. En *El País*. Madrid. Recuperado de: https://elpais.com/tecnologia/2018/05/29/actualidad/1527596274_887116.html
- Rojas, Víctor. (2010). *Derecho internacional público*. México: Nostra Ediciones S. A.
- Savigny, F. (1849). *Tratado de Derecho Romano*. Granada: (s. e.).
- Salmón, Elizabeth. “La globalización de la justicia internacional: hacia un nuevo orden público internacional”. En *Lus et veritas*, año 17, n.° 34, 2007, pp. 245-255.
- Salmón, Elizabeth. “El orden público internacional y el orden público interno desde la perspectiva del Derecho Internacional de los Derechos Humanos”. En *Thémis, Revista de Derecho,* 2, n.° 51, 2005, pp. 151-157.
- Slaugther and May. (2016). “New Rules Wider Reach The Extraterritorial Scope of the GDRP”. Junio. Recuperado de: https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf
- Sánchez, J. M. (2018). “Protección de Datos sanciona a *Whatsapp* y *Facebook* por ceder y tratar datos personales sin consentimiento”. *ABC*. Recuperado de: http://www.abc.es/tecnologia/redes/abci-proteccion-datos-sanciona-whatsapp-y-

facebook-ceder-y-tratar-datos-personales-sin-consentimiento-201803151019_noticia.html

- STC N.° 00146-2015-PHD/TC, del 21 de noviembre de 2017. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2018/00146-2015-HD.pdf
- STC N.° 04729-2011-PDH/TC, del 11 de mayo del 2012. Recuperado de: https://www.tc.gob.pe/jurisprudencia/2013/04729-2011-HD.pdf
- STJUE de fecha 13 de mayo de 2014 (C-131/12) Recuperado de: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES
- STJUE de 6 de octubre de 2015 (Caso 362/14)
- STJUE del 24 de setiembre de 2019 (Caso C-507/17).
- Soler, Israel y William Jiménez. (2014). "¿Cómo establecer la jurisdicción y competencia en casos de internet? Tendencias internacionales y nacionales". En: *Diálogos de saberes: investigaciones y ciencias sociales*, n.º 41, 2014, pp. 15-32. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5467510
- Soto, Daniel. (2010). *Principios Generales del Derecho a la Información*. Toluca: Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Recuperado de: https://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_003_2009.pdf
- Stigall, Dan. (2012). "International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U. S. Domestic Law". En *Hastings International and Comparative Law Review* (Vol. 35, n.°. 2, año 2012. Recuperado de: https://papers.ssrn.com/ sol3/papers.cfm?abstract_id=2043287
- Thuy ong. "Facebook announces new European privacy controls, for the world", *The Verge*, 18 de abril, 2018. Recuperado de: https://www.theverge.com/2018/4/18/17250840/facebook-privacy-protections-europe-world-gdpr

- Tribunal de Justicia de la Unión Europea. Recurso contencioso-administrativo n.° 25/2008 (RJ 2010/6271).
- Varela, Adrian. (2016). "Reconocimiento de sentencias judiciales entre España y EE. UU." *Estudios Institucionales*. (Vol. 3, n.º 4, junio 2016. pp. 217-250). Colombia.
- Vargas, Mónica. (2015). *Extraterritorialidad: Mecanismos de Control Frente a la Vulneración de los Derechos por Empresas Transnacionales*. Observatorio del Deute en la Globalización, pp. 1 y ss.
- Velasco, I. (2011). *Territorialidad, extraterritorialidad e interés.* Recuperado de: www.raco.cat/index.php/InDret/article/download/241332/323923
- Velasco Rico, C. (2018). *Territorialidad, extraterritorialidad e interés Análisis comparado de los sistemas de distribución de competencias de Estados Unidos, Canadá, Austria, Alemania e Italia: lecciones para el Estado Autonómico*. Barcelona. Recuperado de: www.indret.com
- Washington Post. (2018). Recuperado de: https://www.washingtonpost.com/news/ the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.8ecdbd61dcdf
- Wimmer, Kurt. (2018). "Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?" (1 de junio de 2018). Syracuse Law Review, Vol. 68, 2018. Available at SSRN: https://ssrn.com/abstract=3188974