Universidad de
SanAndrés

Universidad de San Andrés

Departamento de Derecho - Maestría en Derecho Empresario

"Transferencia internacional de datos: ¿por qué desafiar el statu quo de la normativa local argentina? Un análisis a partir del marco regulatorio de la Unión Europea"

Autor: Mariana Patricia Fantini

Documento Nacional de Identidad: 36.990.952

Mentor de Tesis: Pablo Iannello

Buenos Aires, 10 de marzo de 2023

Índice

Transferencia internacional de datos: ¿por qué desafiar el statu quo de la normativa local argentina? Un análisis a partir del marco regulatorio de la Unión Europea

Abstract

En las últimas décadas estamos experimentando una continua revolución tecnológica y digital. En este escenario, los datos personales juegan un papel fundamental en el desarrollo de la economía mundial por lo que en los últimos años la recolección e intercambio de datos ha aumentado significativamente. Sin embargo, esta nueva realidad trae consigo también un nuevo reto: contar con una regulación robusta que garantice adecuadamente la protección de estos datos. En la presente tesis se analizará y responderá a la luz de la normativa europea qué aspectos y por qué el statu quo de la normativa argentina que regula la transferencia internacional de datos debiera desafiarse.

I. Introducción

Sin duda en las últimas décadas estamos experimentando una continua revolución tecnológica y digital. La penetración de las recientes innovaciones en la tecnología ha sido increíblemente rápida debido a la evolución y proliferación de las redes móviles y sociales , la inteligencia artificial, la robótica y el internet de las cosas. En esta transición, el término "privacidad" adquiere también una nueva dimensión. Los datos personales, que se recolectan a través de aplicaciones, sitios web, redes inalámbricas móviles, cámaras, micrófonos, etc., comienzan a ser los nuevos protagonistas.

Las empresas privadas y las autoridades públicas en diferentes partes del mundo y a través de distintos tipos de software, procesan y analizan los datos, difuminando las fronteras entre lo público y lo privado. Los datos personales se han convertido en la materia prima que

alimenta a la industria ya que revelan información vinculada con la personalidad, las preferencias y comportamientos de los consumidores. Por lo tanto, cuanto mayor es el bloque de información que las empresas logran recabar, mayor será su éxito a la hora de ofrecer sus servicios. Por su parte, los estados también consideran esta información de vital importancia ya que resultan útiles para fines políticos, por ejemplo, para la defensa y protección de la seguridad nacional.

Los avances en la inteligencia artificial y el volumen masivo de datos han generado que estos procesos sean extremadamente eficaces y es en este contexto de globalización tecnológica es que la transferencia internacional de datos resulta fundamental. El mundo interconectado ha provocado que aquellos datos recabados por empresas y autoridades públicas sean ahora objeto de transferencias internacionales provocando un flujo de datos masivos entre distintas jurisdicciones.

Esta nueva realidad, en el cual millones de datos son transferidos día a día en distintas partes del mundo, trae consigo también un nuevo reto: contar con una regulación robusta que garantice adecuadamente la protección de estos datos y que la misma se encuentre alineada con los estándares internacionales. Ahora bien, es en este punto donde surgen los interrogantes: ¿Argentina cuenta con un régimen normativo robusto y completo que cumpla con un nivel de protección adecuado en lo que respecta a la transferencia internacional de datos?, ¿la regulación europea en esta materia resulta superior a la normativa local argentina?, ¿qué elementos de la normativa europea podrían trasplantarse en nuestra legislación local?, ¿qué conceptos del sistema argentino debieran adecuarse para receptar la normativa europea?

El objetivo principal de esta tesis es examinar y responder qué aspectos y por qué el statu quo de la normativa argentina que regula la transferencia internacional de datos debiera desafiarse. Como objetivos secundarios, se identificarán cuáles son los preceptos de la

normativa europea que podrían trasplantarse a nuestra legislación local y de qué manera estos podrían ser incorporados a nuestro régimen legal.

II. Metodología

A fin de lograr el objetivo propuesto, recurriremos al método funcional comparativo el cual consiste en analizar y comparar dos objetos, en este caso, el marco normativo de la Unión Europea y la normativa local Argentina en materia de protección de datos personales, con el propósito de identificar sus semejanzas y diferencias. Los comparatistas funcionalistas sostienen que los elementos más relevantes de este método son: (i) enfocarse en los efectos fácticos de la regulación, lo que significa que el análisis no se basa en discusiones doctrinales sino en hechos y decisiones judiciales, (ii) este enfoque fáctico debe entenderse en su contexto de aplicación, por lo tanto, se considera que el derecho y la sociedad son separables pero se encuentran vinculados, (iii) las instituciones jurídicas y no jurídicas aun siendo diferentes resultan comparables si cumplen funciones similares en distintos sistemas y (iv) el análisis de la funcionalidad puede resultar útil como criterio evaluativo a fin de identificar cual es "la mejor ley" en tanto esta cumple mejor su función que las demás [1].

En virtud de lo expuesto, en primer lugar, se analizará el marco normativo de la Unión Europea en lo que refiere a la protección de datos personales para luego focalizarnos especialmente en la regulación de las transferencias internacionales de datos. Para ello analizaremos exhaustivamente el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea de fecha 27 de abril de 2016. Luego, de modo de examinar la normativa europea de manera integral y desde una perspectiva fáctica, analizaremos la sentencia del Tribunal de Justicia de la Unión Europea de fecha 16 de julio de 2020, dictada en el asunto C-311/18, también conocida como "Schrems II". Las consideraciones de este fallo

[1] Michaels, Ralf (2006), "The Functional Method of Comparative Law", Publicado en: The Oxford Handbook of Comparative Law, Paper No. 87. Disponible en inglés en el siguiente enlace: SSRN: https://ssrn.com/abstract=839826.

resultan sumamente relevantes en lo que respecta a la protección y transferencia internacional de datos en tanto analiza varias aristas de la regulación europea que impactan en la circulación de los datos personales entre la Unión Europea y los terceros países. Una vez determinadas las características principales del sistema normativo europeo y habiendo analizado su correspondiente aplicación, concluiremos esta primera parte detallando por qué el sistema normativo europeo está a la vanguardia en materia de protección de datos.

Posteriormente revisaremos la normativa local argentina en lo que respecta a la protección de datos personales para luego focalizarnos en la regulación de las transferencias internacionales de datos. Para ello, revisaremos la Ley de Protección de Datos Personales N.º 25.326, el Decreto N.º 1558/2001, la Disposición 60/2016, y la Ley de Acceso a la Información Pública N.º 27.275.

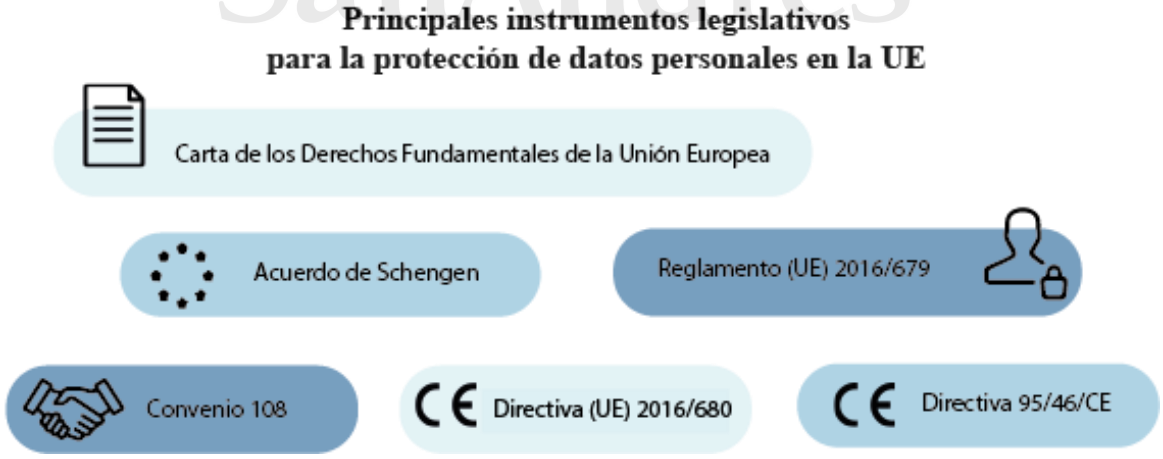
Una vez examinadas las características propias de ambos regímenes legales, su aplicación práctica y sus instituciones se nos permitirá analizar el trasplante legal, el cual consiste en el traspaso de leyes e instituciones legales entre los distintos Estados[2].Desde esta base teórica, se concluirá la presente tesis con la identificación de los preceptos y las herramientas más idóneas provistas por el marco regulatorio europeo en materia de

[2] Al respecto, cabe tener presente que de acuerdo a las motivaciones que impulsan su adopción, los trasplantes legales puede clasificarse en: (i) el Trasplante que ahorra costos, en el cual el legislador a fin de resolver un problema en lugar de diseñar por sí mismo la solución, importa una solución ya aplicada en un país extranjero, ahorrando de este modo el costo que genera el desarrollo de legislación y los estándares regulatorios; (ii) el Trasplante determinado desde el exterior, el cual involucra la adopción de un modelo legal extranjero a fin de expandirse y tener la posibilidad de generar negocios con ese tercer país; (iii) el Trasplante entrepreneur, el cual refiere a aquellas personas que estudian un modelo extranjero y luego alientan su adopción en el sistema local; y (iv) el Trasplante que genera legitimidad, el cual consiste en la importación de un modelo foráneo con prestigio generando que este obtenga una mayor autoridad legal y aceptación. Tal como se desarrollará en la presente exposición, en la práctica estos tipos de trasplantes se mezclan y no resulta usual encontrar uno en su forma pura. Ello conforme Miller, Jonathan M. (2006), "Una tipología de los trasplantes legales: utilizando la sociología, la historia del derecho y ejemplos argentinos para explicar el proceso de trasplante", Publicado en Lecciones y ensayos Nº 81. Disponible en español el siguiente enlace: http://www.derecho.uba.ar/publicaciones/lye/revistas/81/una-tipologia-de-los-transplantes-legales.pdf.

transferencia internacional de datos para luego examinar por qué estos debieran exportarse e incorporarse en el régimen legal argentino.

III. Legislación europea en materia de protección de datos personales

La Unión Europea posee una larga tradición de protección a la privacidad y ha sido históricamente pionera en la protección de datos personales. El auge de la economía digital entendida como "*la red mundial de actividades económicas y transacciones comerciales habilitadas por las tecnologías de la información y la comunicación*"[3] y el gran volumen de datos que se producen como consecuencia de estas transacciones y el intercambio de información mediante redes, trajo consigo un nuevo desafío: crear un régimen capaz de resguardar los datos personales. Tal como surge a continuación, en el transcurso del tiempo, en la medida en que se expandieron las nuevas tecnologías, aumentaron también las herramientas y garantías ofrecidas por la regulación con el afán de adaptarse y actualizarse a estas innovaciones tecnológicas. A continuación revisaremos brevemente la evolución de la normativa europea reflejada en los principales instrumentos legislativos indicados en la Figura 1[4].



[3] Trevisán, Pablo (2022): "Competencia, datos y economía digital", Publicado en: LA LEY 20/09/2022, 1, Cita: TR LALEY AR/DOC/2726/2022.
[4] Principales instrumentos legislativos para la protección de datos personales en la UE.

i. Convenio 108

En primer lugar cabe mencionar al Convenio 108 del Consejo de Europa, adoptado el 28 de enero de 1981 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal[5], ya que se trata del primer instrumento internacional jurídicamente vinculante sobre protección de datos[6]. Este convenio admitió la necesidad de que los países que conforman la Unión Europea trabajen en encontrar una regulación uniforme para asegurar a nivel regional una protección homogénea de los datos personales a través del cumplimiento de determinados principios que aun hoy siguen siendo los cimientos de esta materia[7]. En este sentido, protege el derecho a la privacidad con respecto al tratamiento automatizado de los datos de carácter personal y establece las bases para la protección de datos. A saber: (a) los datos deben ser recogidos y procesados de manera legítima y lícita y, su período de conservación debe ser razonable, (b) los datos sensibles debe estar sujetos a un tratamiento especial, (c) se deben tomar las medidas de seguridad necesarias para garantizar la protección adecuada de datos y (d) las personas tienen derecho a conocer que sus datos están siendo procesados, los propósitos de ello y deben conversar los derechos de acceso, rectificación y supresión.

[5] Disponible en inglés en el siguiente enlace: https://rm.coe.int/1680078b37. Este instrumento se ha actualizado en el año 2018 mediante el Convenio 108+ a fin de adaptar la normativa a los avances tecnológicos e incorporar nuevos principios esenciales para la protección de datos.

[6] De acuerdo con la exposición de motivos de la Propuesta de la Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108) de fecha 5 de junio de 2018, 51 Estados han ratificado el Convenio 108, incluida la totalidad de los 28 Estados miembros de la UE, los cuatro Estados de la AELC, todos los países de los Balcanes Occidentales, varios países vecinos (por ejemplo, Armenia y Georgia), la Federación de Rusia, Turquía y varios países no europeos de África (por ejemplo, Senegal y Túnez) y Latinoamérica (Uruguay). Varias solicitudes de adhesión (por ejemplo, Argentina, México y Marruecos) están en curso y varios países tienen calidad de observador (por ejemplo, Japón y Corea del Sur). Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0451&from=LT#:~:text=En%20la%20actualidad%2C%2051%20Estados,varios%20pa%C3%ADses%20no%20europeos%20de.

[7] Basavilbaso, Marina (2022): "Régimen argentino de protección de datos personales", Publicado en: RCCyC 2022 (abril), 05/04/2022, 5 Cita: TR LALEY AR/DOC/771/2022.

ii. Acuerdo de Schengen

En segundo lugar, es importante mencionar al Convenio de aplicación del Acuerdo de Schengen de fecha 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes[8] ya que establece una serie de medidas para que exista una estrecha cooperación entre las partes contratantes e incluye y regula especialmente en su Título VI la protección de los datos de carácter personal en lo que respecta a la transmisión de datos entre los estados miembros y a su tratamiento automatizado.

iii. Directiva 95/46/CE

Asimismo, resulta importante señalar la Directiva 95/46/CE (1995) del Parlamento Europeo y del Consejo de 24 de octubre de 1995[9] cuyo objetivo fue proponer una legislación supranacional que alineó todas las normas locales sobre protección de datos, la cual era sumamente necesaria para los Estados que conforman la Unión Europea. Al respecto, cabe decir que si bien esta norma uniformó a las distintas legislaciones de los Estados miembros, por otro lado también acotó su margen de actuación en tanto estos debieron adaptar sus normativas locales. En lo que respecta a la transferencia de datos hacia países extracomunitarios, esta Directiva estableció ciertas reglas que debían cumplir dichas naciones para poder ser consideradas "países adecuados", lo que permitiría a estos estados que no pertenecían a la Unión Europea ejecutar transferencias sin requisitos adicionales[10].

[8] Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:42000A0922(02)&from=ES.

[9] Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES.

[10] Velázquez, Jorge D. (2019): "Protección de datos: Una nueva era en la cultura de la privacidad" Publicado en: SJA 03/04/2019, 53 - Cita: TR LALEY AR/DOC/1170/2019.

Asimismo, impuso que los Estados miembros designen una o más autoridades públicas para vigilar la aplicación de esta norma en su territorio, quienes conservarán poderes de investigación y de capacidad procesal[11].

iv. Carta de los Derechos Fundamentales de la Unión Europea

Además, resulta relevante tener presente a la Carta de los Derechos Fundamentales de la Unión Europea[12], un instrumento internacional que por primera vez reconoce expresamente como derechos fundamentales el respeto de la vida privada (artículo 7) y la protección de los datos de carácter personal (artículo 8), estableciendo que los datos deben ser tratados de forma 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. Asimismo, dispone que toda persona conserva el derecho a acceder a sus datos y a la correspondiente rectificación.

v. Reglamento (UE) 2016/679

Asimismo, cabe destacar al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea de fecha 27 de abril de 2016 (conocido como Reglamento General de Protección de Datos, en adelante "RGPD" o el "Reglamento")[13], que sustituyó a la Directiva 95/46/CE descripta más arriba y exacerbó el régimen de protección de datos atento que en el marco del crecimiento de las nuevas tecnologías, el gran flujo de información y el Internet de las Cosas[14], la infracción de datos aumentaría sin una legislación adecuada[15]. Este

[11] Artículo 28 "Autoridad de control".
[12] Disponible en español en el siguiente enlace: text_es.pdf (europa.eu).
[13] Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=es.
[14] Término que se utiliza para referirse a aquellos objetos físicos que tienen incorporados cierta tecnología que permite que estos se encuentren conectados a internet y que, en consecuencia, reciban y transfieran datos.
[15] Weber, Rolf H. (2017): "Transnational Data Privacy in the EU Digital Single Market Strategy", Publicado en Privacy and Transborder Flows of Personal Data, pp. 5 – 26, Cambridge University Press.

texto formado por 173 considerandos, 99 artículos se publicó en el Diario Oficial de la Unión Europea el 4 de mayo de 2016 y entró en vigencia el 25 de mayo de 2018 y, tiene como objetivos principales: (i) garantizar el derecho fundamental de protección de las personas físicas en relación con el tratamiento de sus datos personales, (ii) establecer un nivel uniforme y elevado de protección para que la regulación sea equivalente en todos los Estados miembros de la Unión Europea y, de este modo, crear un sistema normativo coherente y homogéneo, (iii) eliminar los obstáculos a la circulación de datos personales dentro de la Unión Europea (en adelante "UE", "Unión" o "Unión Europea")[16]. El propósito principal es que todos los Responsables, o Encargados de tratamiento de datos respeten el principio de Responsabilidad proactiva lo que implica que las organizaciones revisen qué datos tratan, analicen los fines y qué tipo de operaciones de tratamiento realizan para luego explicar a la Autoridad de Control como implementan la regulación[17].

Asimismo, cabe señalar este Reglamento tiene un impacto significativo debido principalmente a: (i) su extraterritorialidad y (ii) la imposición de sanciones importantes[18].

vi. Directiva (UE) 2016/680

Finalmente, es relevante mencionar la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de fecha 27 de abril de 2016[19], la cual resguarda el derecho fundamental

[16] Para más información revisar los considerandos del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.
[17] Guini, Leonor (2020): "Guía de Evaluación de Impacto en la protección de datos", Publicado en: SJA 08/07/2020, 87 - Cita: TR LALEY AR/DOC/1977/2020.
[18] Abdelnabe Vila, María C. - Cisilino, Arnaldo (2020): "Perspectivas de la Protección de Datos Personales: status quo y proyecciones", Publicado en: SupAbCorp 2020 (noviembre), 27/11/2020, 1 Cita: TR LALEY AR/DOC/3772/2020. El artículo 83 del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea establece importantes multas administrativas de hasta 10.000.000 euros o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía o ante casos graves hasta 20.000.000 de euros o hasta el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.
[19] Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de

de los ciudadanos a la protección de datos cuando estos sean utilizados por las autoridades encargadas de velar por el cumplimiento de la ley. En particular, garantiza que los datos personales de las personas implicadas en procesos penales tales como víctimas, testigos y sospechosos de delitos sean debidamente protegidos, y facilita la cooperación transfronteriza, en especial en materia de lucha contra el terrorismo y la delincuencia.

IV. Transferencias internacionales de datos: marco normativo de la Unión Europea

Tal como hemos mencionado, la revolución tecnológica y la globalización han planteado nuevos desafíos a la hora de proteger los datos personales y uno de ellos se encuentra vinculado con el hecho de que actualmente una gran parte del comercio involucra el tratamiento de los datos personales de los ciudadanos europeos, atento que numerosas compañías dependen del acceso a dichos datos para ofrecer sus servicios[20]. Asimismo, muchos proveedores de servicios que desarrollan su actividad a usuarios europeos/consumidores, tienen su establecimiento fuera de la UE, mientras que los servidores donde se encuentran los centros de almacenamiento de los datos se sitúan en otro u otros Estados diferentes[21]. En este contexto es que la recolección y transferencia masiva de datos por parte de entidades públicas y privadas ha generado la necesidad de regular la circulación de datos dentro de la Unión Europea, así como también en lo que respecta a las transferencias a terceros países y a organizaciones internacionales, incluyendo además a aquellas transferencias ulteriores desde los países extracomunitarios. En este escenario el marco jurídico del Derecho europeo provee

dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Disponible en español el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES.

[20] Sobrino García, I. (2021): "Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos", Revista de Derecho Comunitario Europeo, 68, 227-256. doi: https://doi.org/10.18042/cepc/rdce.68.07.

[21] Cordero Álvarez, Clara Isabel (2019): "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: especial referencia al caso estadounidense y la Cloud Act", Revista Española de Derecho Europeo, 70, pp. 49-108.

distintas herramientas en las que si bien tiene reconoce que el flujo de datos personales es esencial para la expansión del comercio, ello no debe suponer que las transferencias puedan ejecutarse violando los derechos de los usuarios y menoscabando el nivel de protección adecuado[22].

A fin de comprender el alcance de este Reglamento, se detallará a continuación el ámbito de aplicación material y territorial y, se proveerá una breve introducción sobre las definiciones más relevantes que deben tenerse presente. Estos puntos resultan esenciales para el entendimiento de esta exposición ya que el alcance de los conceptos que se desarrollarán aquí debajo nos permitirán identificar en que supuestos el RGPD resulta aplicable.

En lo que respecta al ámbito material, el Reglamento determina que resultará aplicable "*al tratamiento total o parcialmente automatizado de datos personales, así como también al tratamiento no automatizado de datos personales cuando estos estén o vayan a estar incluidos en un fichero*"[23].

En cuanto al ámbito territorial, el RGPD será de aplicación a aquellos establecimientos[24] que traten datos personales y tengan su sede en la UE, independientemente de dónde se traten de hecho los datos. También se aplicará a aquellos establecimientos que tengan su sede fuera de la UE pero cuyo tratamiento de datos esté vinculado con: (i) ofertas de bienes o servicios a ciudadanos en la UE (independientemente de si a estos se les requiere su pago), o (ii) supervisan el comportamiento de ciudadanos en la UE. Concretamente, el RGPD tiene un impacto potencial en cualquier compañía del mundo que haga tratamiento de datos de

[22] Considerando 101 del RGPD.
[23] Artículo 2: "Ámbito de aplicación material" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea. Asimismo, este artículo provee un detalle expreso sobre aquellas situaciones en las que el Reglamento no resultará aplicable.
[24] El considerando 22 del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea dispone: "*un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto*". Como se observa la norma ofrece una definición amplia de este término y determina que deben analizarse los elementos fácticos por sobre los aspectos legales.

residentes europeos o preste bienes o servicios a residentes de la Unión[25]. Por último, también alcanzará al tratamiento de datos personales por parte de un responsable que esté establecido en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público[26].

En relación a las definiciones que resultan relevantes para el presente análisis, cabe mencionar que de acuerdo al artículo 4: (i) se entenderá por "datos personales" a toda la información sobre una persona física identificada o identificable[27]; (ii) el alcance de la palabra "tratamiento" será cualquier operación o conjunto de operaciones realizadas sobre datos personales tales como la recogida, conservación, adaptación o extracción, entre otros; (iii) será considerado "responsable del tratamiento" aquella persona física o jurídica, autoridad pública, servicio u otro organismo que determine los fines y medios del tratamiento y; (iv) "encargado del tratamiento" será la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Ahora bien, en lo que respecta a la transferencia internacional de datos, el capítulo V del RGPD provee un complejo régimen normativo atento que propone una serie de mecanismos que permiten ejecutar las transferencias de datos personales a terceros países u organizaciones internacionales garantizando un adecuado nivel de protección. En tal sentido, dispone que solamente se podrán hacer aquellas transferencias en las que el responsable y el encargado del tratamiento cumplan con las condiciones descriptas en el RGPD, incluyendo

[25] Frene, Lisandro (2018): "Reglamento General de Protección de Datos de la Unión Europea. Extraterritorialidad e impacto en Argentina", Publicado en: LA LEY 06/09/2018, 1 – LA LEY2018-E, 1275 Cita: TR LALEY AR/DOC/1764/2018.

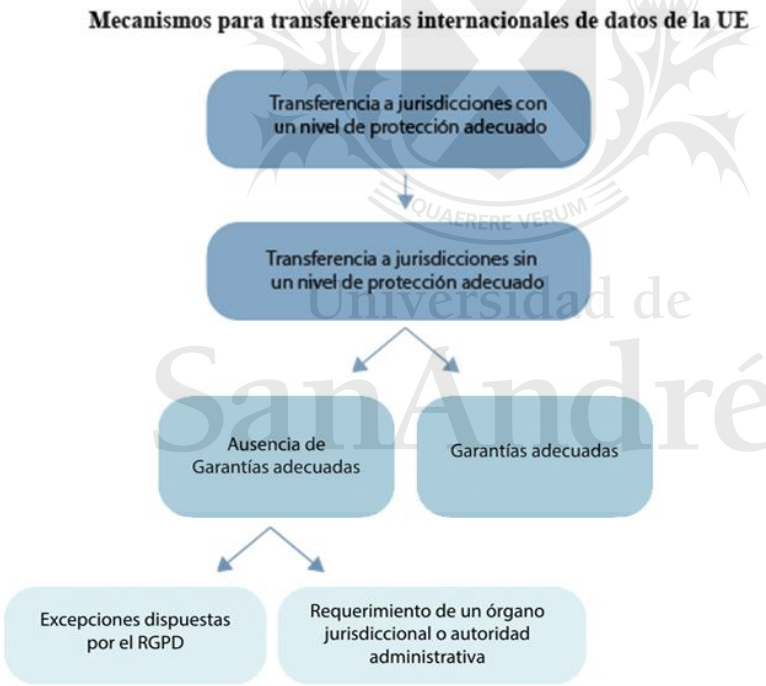
[26] Artículo 3: "Ámbito territorial" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

[27] Una persona física se considerará identificable cuando pueda determinarse su identidad directa o indirectamente, por ejemplo a través de su nombre, número de identificación, datos de localización, entre otros factores identificados por la propia norma.

aquí también las transferencias ulteriores desde el tercer país u organización internacional a otro tercer país u otra organización internacional[28].

Previo a desarrollar exhaustivamente cada uno de los métodos previstos por el Reglamento, cabe aclarar que el RGPD resulta también aplicable a Islandia, Liechtenstein y Noruega. Ello se debe a que el RGPD se incluyó en el Acuerdo sobre el Espacio Económico Europeo[29] (en adelante "EEE"). En virtud de ello, las transferencias realizadas entre los estados miembros del EEE no serán consideradas como transferencias internacionales y en consecuencia, los datos circularán libremente como si se tratara de un solo estado.

A continuación, se describirán los distintos mecanismos establecidos por el RGPD para las transferencias internacionales de datos, indicados en la Figura 2[30].



[28] Artículo 44: "Principio general de las transferencias" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.
[29] Este acuerdo incluye todos los países de la UE y a Islandia, Liechtenstein y Noruega y, tiene como finalidad posibilitar la libre circulación de bienes, servicios, capitales y personas.
[30] Mecanismos para transferencias internacionales de datos de la UE.

i. Transferencias basadas en una decisión de adecuación

La primera alternativa que habilita el RGPD es la transferencia de datos personales a un tercer país, territorio o sector u organización internacional que la Comisión Europea (en adelante la "Comisión") haya resuelto, con efectos para toda la UE, que ese tercer país, territorio o sector del tercer país, o la organización internacional garantiza un nivel de protección adecuado. Esta decisión permite la libre circulación de los datos personales hacia ese tercer país sin que sea necesario aportar garantías adicionales, ni obtener ningún tipo de autorización específica[31]. Se trata entonces de un instrumento jurídico esencial que autoriza la libertad de flujo transfronterizo de datos[32]. De esta forma, la Comisión garantiza en la Unión seguridad y uniformidad jurídica en lo que se refiere al tercer país, sector u organización internacional que se considere que ofrece tal nivel de protección[33].

A tal fin el RGPD detalla de manera precisa cuales son los factores que deberá considerar la Comisión para evaluar la adecuación de protección. Para ello, analizará criterios objetivos, a saber: (a) las circunstancias propias de ese territorio como por ejemplo la legislación pertinente y su aplicación, la jurisprudencia, si los titulares de los datos tienen derechos efectivos y exigibles y, cuentan con recursos administrativos y acciones judiciales que sean efectivos; (b) la existencia y el funcionamiento de las autoridades de control

[31] Artículo 45: "Transferencias basadas en una decisión de adecuación" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

[32] Andoni Polo Roca (2021): "Las transferencias internacionales de datos: regulación actual y su incidencia en las relaciones exteriores de la Unión Europea". Publicado en: Revista Aragonesa de Administración Pública ISSN 2341-2135, núm. 57, Zaragoza, 2021, pp. 325-369.

[33] Conforme considerando 103 del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea. Cabe destacar que la principal diferencia entre el Reglamento y la anterior Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 es que este nuevo régimen propone como exclusiva autoridad parar declarar la idoneidad del país de destino de la transferencia por ser adecuado su nivel de protección es la Comisión; sin que se haga referencia que tal posibilidad pudiera recaer a los Estados Miembros, conforme se permitía en el artículo 25 de la mencionada Directiva.

independientes, y (c) los compromisos internacionales u otras obligaciones vinculantes asumidas por ese tercer país u organización internacional[34].

La Comisión además establecerá un mecanismo de control para analizar los acontecimientos relevantes que puedan alterar la adecuación y, de ser necesario, se encontrará facultada para modificar su decisión (sin efecto retroactivo) previa declaración motivada. Asimismo, publicará en el Diario Oficial de la Unión Europea y en su página web una lista que detalla los terceros países, sectores, y organizaciones internacionales que garantizan un nivel de protección adecuado[35].

Recientemente la Comisión resolvió la aplicación de este mecanismo para la ejecución de transferencias internacionales de datos entre la Unión Europea y el Reino Unido. La salida del Reino Unido de la UE[36] implica también que este deja de formar parte del EEE y en consecuencia, ya no goza de la libre circulación de bienes, servicios, capitales y personas entre los distintos países que conforman el EEE. En virtud de lo expuesto, el Reino Unido comienza a ser considerado un tercer país a efectos del RGPD lo que implica que las transferencias

[34] Para mayor detalle por favor revisar el artículo 45: "Transferencias basadas en una decisión de adecuación" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

[35] Acceso a la lista aprobada hasta la fecha (31 de mayo de 2022) de los países y territorios declarados como adecuados:https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[36] También conocido como el "Brexit", un acrónimo de dos palabras en inglés: *"Britain" y "exit",* que hace referencia a la salida del Reino Unido de la Unión Europea, luego de que los ciudadanos británicos se pronunciaran a favor de la retirada de la UE en el Referéndum celebrado el 23 de junio de 2016. De acuerdo con el artículo 50 del Tratado de la Unión Europea cualquier Estado miembro podrá retirarse de la Unión Europea en caso que así lo desee. Para ello deberá notificar al Consejo Europeo sobre su intención y deberá negociar por un plazo máximo de dos años un acuerdo de retirada, en el cual se determinará el marco de la futura relación entre ese Estado y la UE, de acuerdo con los lineamientos establecidos en el artículo 218, apartado 3, del Tratado de Funcionamiento de la Unión Europea. El artículo mencionado reza lo siguiente: "*La Comisión, o el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad cuando el acuerdo previsto se refiera exclusiva o principalmente a la política exterior y de seguridad común, presentará recomendaciones al Consejo, que adoptará una decisión por la que se autorice la apertura de negociaciones y se designe, en función de la materia del acuerdo previsto, al negociador o al jefe del equipo de negociación de la Unión*".

realizadas entre los estados miembros del EEE y el Reino Unido sean consideradas transferencias internacionales y que los datos ya no circulen libremente[37].

Luego de culminar el análisis sobre el marco normativo del Reino Unido, el 28 de junio de 2021 la Comisión decretó formalmente que a los efectos de lo establecido en el artículo 45, apartado 3, del Reglamento (UE) 2016/679[38], el Reino Unido mantiene un adecuado nivel de protección[39]. Para así resolver, la Comisión tomó en consideración que previo a la salida y durante todo el período transitorio, el marco regulatorio sobre la protección de datos personales del Reino Unido consistía en la legislación de la UE ya que dentro de la normativa local británica, el Data Protection Act de 2018 (DPA de 2018)[40], incorporó la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016. Asimismo, tuvo presente que incluso una vez efectivizada la retirada, el marco jurídico sobre la protección de datos personales en el Reino Unido se mantuvo basada en la legislación de la UE y por lo tanto, los principales lineamientos delineados por la normativa europea se encontraban incluidos[41].

[37] No obstante, cabe aclarar que el RGPD sigue y seguirá siendo aplicable en muchas empresas del Reino Unido dada su aplicación extraterritorial tal como hemos explicado más arriba (ver punto "IV. Transferencias internacionales de datos: marco normativo de la Unión Europea" en lo que respecta al ámbito de aplicación).

[38] Este artículo establece que la Comisión puede decidir, mediante un acto de ejecución, que un tercer país garantiza un nivel de protección adecuado.

[39] Ello mediante la Decisión de ejecución (UE) 2021/1773 de la Comisión de 28 de junio de 2021 con arreglo a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por parte del Reino Unido. Disponible en español en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32021D1773&from=ES

[40] El Data Protection Act de 2018 es una ley del Reino Unido que entró en vigor el 23 de mayo de 2018 que regula la protección de datos y complementa la aplicación del RGPD. Disponible en el siguiente enlace: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[41] Cabe aclarar que esta Decisión de Ejecución será aplicable durante un período de cuatro años a partir de su entrada en vigor. Es decir que tendrá validez hasta el 27 de junio de 2025. Asimismo, la Comisión hará una revisión continua de hecho y de derecho para determinar si se mantienen los parámetros necesarios para que exista una protección adecuada.

Hasta la fecha[42], la Comisión también ha reconocido que mantienen un adecuado nivel de protección los siguientes territorios: Andorra[43], Argentina[44], Canadá (organizaciones internacionales)[45], Islas Feroe[46], Guernsey[47], Israel[48], Isla de Man[49], Japón[50], Jersey[51], Nueva Zelanda[52], República de Corea[53], Suiza[54] y Uruguay[55].

[42] 31 de mayo de 2022.

[43] Decisión de la Comisión (2010/625/UE) de 19 de octubre de 2010 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra [notificada con el número C(2010) 7084].

[44] Decisión de la Comisión (2003/490/CE) de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

[45] Decisión de la Comisión (2002/2/CE) de 20 de diciembre de 2001con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación dela protección de los datos personales conferida por la ley canadiense Personal Information and Electronic Documents Act [notificada con el número C(2001) 4539].

[46] Decisión de la Comisión (2010/146/UE) de 5 de marzo de 2010 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales [notificada con el número C(2010) 1130].

[47] Decisión de la Comisión (2003/821/CE) de 21 de noviembre de 2003 relativa al carácter adecuado de la protección de los datos personales en Guernsey [notificada con el número C(2003) 4309].

[48] Decisión de la Comisión (2011/61/UE) de 31 de enero de 2011 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales [notificada con el número C(2011) 332].

[49] Decisión de la Comisión (2004/411/CE) de 28 de abril de 2004 relativa al carácter adecuado de la protección de los datos personales en la Isla de Man [notificada con el número C(2004) 1556].

[50] Decisión de Ejecución (UE) 2019/419 de la Comisión de 23 de enero de 2019 con arreglo al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativa a la adecuación de la protección de los datos personales por parte de Japón en virtud de la Ley sobre la protección de la información personal [notificada con el número C(2019) 304].

[51] Decisión de la Comisión (2008/393/CE) de 8 de mayo de 2008 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey [notificada con el número C(2008) 1746].

[52] Decisión de Ejecución de la Comisión (2013/65/UE) de 19 de diciembre de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda [notificada con el número C(2012) 9557].

[53] Decisión de Ejecución de la Comisión de 17 de diciembre de 2021 de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo sobre la protección adecuada de los datos personales por parte de la República de Corea en virtud del Ley de protección de datos personales

[54] Decisión de la Comisión (2000/518/CE) de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza[notificada con el número C(2000) 2304].

[55] Decisión de Ejecución de la Comisión (2012/484/UE) de 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales [notificada con el número C(2012) 5704].

ii. Transferencias mediante garantías adecuadas

La segunda alternativa propuesta por el RGPD, en ausencia de una decisión de la Comisión por la que se constate la adecuación de la protección de los datos, es que el responsable o encargado del tratamiento solo podrá realizar la transferencia de datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas de protección de datos y siempre que los usuarios cuenten con derechos exigibles y acciones legales efectivas[56], lo que implica el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión Europea o en un tercer país.

Estas garantías pueden ser aportadas a través de las distintas formas establecidas por la propia regulación. A saber: (i) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; (ii) normas corporativas vinculantes de acuerdo con los lineamientos establecidos por el RGPD[57]; (iii) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen establecido por el RGPD[58]; (iv) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión respetando el procedimiento de examen establecido por el RGPD[59]; (v) un

[56] Artículo 46: "Transferencias mediante garantías adecuadas" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

[57] Artículo 47: "Normas corporativas vinculantes" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea. Estas normas son políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta y deben ser: (i) jurídicamente vinculantes, (ii) deben aplicarse y cumplirse por todos los miembros correspondientes del grupo empresarial (entendido cómo grupo constituido por una empresa que ejerce el control y sus empresas controladas) o de la unión de empresas dedicadas a una actividad económica conjunta incluyendo también a los empleados. Asimismo, cabe agregar que al momento de crear estas normas, se deben considerar e incluir ciertos elementos dispuestos por la propia normativa.

[58] El Artículo 93 "Procedimiento de comité", apartado 2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea establece los lineamientos que deben seguirse para cumplir con este método. Para ello dispone la aplicación del artículo 5 del Reglamento (UE) 182/2011. Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011R0182&from=ES.

[59] El Artículo 93 "Procedimiento de comité", apartado 2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea establece los lineamientos que deben seguirse para cumplir

código de conducta junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados[60] (en este caso, serán las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento quienes podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del RGDP[61]); (vi) un mecanismo de certificación junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados[62].

Asimismo y a condición de que exista autorización de la autoridad de control competente, las garantías además pueden ser aportadas mediante: (i) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos

con este método. Para ello dispone la aplicación del artículo 5 del Reglamento (UE) 182/2011. Para su acceso por favor revisar nota del pie anterior.

[60] Existen las siguientes decisiones de la Comisión sobre cláusulas tipo: la Decisión 2001/497/CE de la Comisión de 15 de junio de 2001 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país, la Decisión 2004/915/CE de la Comisión de 27 de diciembre de 2004 relativa a las transferencias entre responsables del tratamiento, y la Decisión 2010/87/UE de la Comisión de 5 de febrero de 2010 relativas a las transferencias de responsables del tratamiento a encargados del tratamiento. Sin embargo, la Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 estableció que las cláusulas contractuales de la decisiones anteriormente mencionadas quedarán derogadas a partir del 27 de septiembre de 2021; si bien los contratos celebrados antes de dicha fecha con arreglo a las decisiones 2001/497/CE o 2010/87/UE se considerarán que ofrecen garantías adecuadas previo al RGPD hasta el 27 de diciembre de 2022, a condición de que las operaciones de tratamiento permanezcan inalteradas y que las cláusulas contractuales tipo garanticen que la transferencia de datos personales esté sujeta a garantías adecuadas.

[61] En lo que respecta por ejemplo a: (i) el tratamiento leal y transparente; (ii) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos; (iii) la recogida de datos personales; (iv) la seudonimización de datos personales; (v) la información proporcionada al público y a los interesados; (vi) el ejercicio de los derechos de los interesados; (v) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño; (vi) las medidas y procedimientos que deben aplicar los responsables del tratamiento para garantizar seguridad; (v) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados; (vi) la transferencia de datos personales a terceros países u organizaciones internacionales, o (vii) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos.

[62] La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación.

personales en el tercer país u organización internacional, o (ii) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. Cabe destacar que el responsable o el encargado del tratamiento que recurra a cláusulas tipo de protección de datos podrá agregar cláusulas o garantías adicionales, a condición de que estas no contradigan los derechos o afecten las libertades fundamentales de los interesados, ni tampoco afecten los derechos y/o garantías establecidas por el Reglamento.

iii. Transferencias o comunicaciones no autorizadas por el Derecho de la Unión y excepciones para situaciones específicas

La tercera opción que dispone el RGPD (en ausencia de una decisión de adecuación de conformidad o de garantías adecuadas) es la transferencia internacional de datos requerida por una sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país siempre que esta se realice en el marco de un acuerdo internacional vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otras motivaciones establecidas por la normativa a la luz del capítulo V de la RGPD[63].

Asimismo, la regulación establece determinadas excepciones para situaciones específicas y dispone que se encuentran permitidas las transferencias internacionales cuando: (a) el interesado dio explícitamente su consentimiento conociendo los posibles riesgos involucrados[64]; (b) esta es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales solicitadas por el interesado; (c) esta es necesaria para la celebración o ejecución de un contrato, en beneficio del

[63] Artículo 48: "Transferencias o comunicaciones no autorizadas por el Derecho de la Unión" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

[64] Al respecto cable aclarar que conforme artículo 4 inciso 11 del del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea, el consentimiento del interesado deberá consistir en "*una manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*".

interesado, entre el responsable del tratamiento y otra persona física o jurídica; (d) esta es necesaria por interés público, para formar, ejercer o defender reclamaciones, para proteger intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento; y (e) esta se realice desde un registro público en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta[65].

Por último, cabe agregar que cuando una transferencia no pueda basarse conforme las alternativas descriptas en los puntos anteriores y tampoco resulte aplicable ninguna de las disposiciones detalladas en el párrafo anterior, la transferencia solamente podrá ejecutarse si: (a) no es repetitiva, (b) afecta a un número limitado de interesados, (c) es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y (d) el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. En este escenario, el responsable del tratamiento también informará a la autoridad de control sobre la transferencia e comunicará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos[66].

V. De la teoría a la práctica: análisis del Asunto C-311/18 – Sentencia del Tribunal de Justicia de la Unión Europea

A fin de examinar la implementación de los mecanismos de transferencia propuestos por el RGDP, en este punto analizaremos la sentencia de la Gran Sala del Tribunal de Justicia de la Unión Europea (en adelante el "TJUE") dictada en el asunto C-311/18, conocida como

[65] En este caso, la transferencia no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Artículo 49: "Excepciones para situaciones específicas" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

[66] Artículo 49: "Excepciones para situaciones específicas" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de la Unión Europea.

"Schrems II"[67], la cual invalidó la Decisión de la Comisión Europea 2016/1250 sobre la adecuación de la protección conferida por el denominado "Privacy Shield"[68] en virtud de la cual se llevaban a cabo las transferencias de datos personales entre la Unión Europea y Estados Unidos. Las consideraciones del fallo resultan sumamente relevantes en tanto analizan determinados aspectos del RGPD que impactan en la transferencia internacional de datos entre la Unión Europea y los terceros países que no han sido reconocidos como adecuados por la Comisión. Para ello, examina la aplicación de la normativa europea y destaca los requisitos mínimos que deben revisarse y cumplirse previo a ejecutar las transferencias internacionales de datos.

A fin de comprender las motivaciones del TJU, a continuación se hará un breve repaso sobre los antecedentes del caso, luego se detallarán cada una de las observaciones y cuestiones prejudiciales presentadas por el Tribunal Superior de Irlanda junto con los respectivos fundamentos ofrecidos por el TJU para resolver de ese modo.

i. Antecedentes

Este caso tiene su origen en el año 2013, cuando el Sr. Maximillian Schrems, residente austríaco y usuario de la red social Facebook, inició un reclamo ante el Comisario para la Protección de Datos de Irlanda (en adelante el "Comisario") para que se le prohibiese a Facebook Ireland transferir sus datos personales a Facebook Inc. Cabe aclarar que al momento de inscribirse en esta red social, el Sr. Schrems celebró un contrato con Facebook Ireland (cuya casa matriz es Facebook Inc.) y cuyos términos y condiciones establecían que los datos personales de los usuarios de Facebook que residan en la Unión Europa se transferirían total o parcialmente a servidores pertenecientes a Facebook Inc., los cuales se encontraban ubicados en el territorio de Estados Unidos y que eran objeto de tratamiento en dicha jurisdicción.

[67] Disponible en español el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62018CJ0311&from=es.
[68] En español conocido como "Escudo de la Privacidad UE EE. UU.".

En el contexto descripto, el cuestionamiento del Sr. Schrems se fundamentó en que las prácticas en vigor de EE.UU. no aseguraban una protección suficiente de los datos personales almacenados en ese territorio frente a las actividades de vigilancia ejercidas por las autoridades públicas de ese país. Dicho reclamo fue desestimado basándose en que la Comisión Europea ya había declarado, en su Decisión 2000/520 CE[69], que Estados Unidos ofrecía un nivel de protección adecuado debido a la existencia de un acuerdo entre el Departamento de Comercio de Estados Unidos y la Unión Europea, que reglamentó la forma en que las empresas estadounidenses podrían realizar la trasferencia de datos personales de los ciudadanos europeos. Este acuerdo es conocido como "Safe Harbour" (en español "Puerto Seguro")[70].

Ante este escenario, el Sr Schrems presentó un recurso contra la desestimación de su reclamo y planteó al Tribunal Superior de Irlanda una petición de decisión prejudicial sobre la interpretación y validez de la Decisión 2000/520/CE.

En octubre de 2015, el Tribunal de Justicia a través de la sentencia C 362/14, EU:C:2015:650 (conocida como "Schrems I")[71], declaró inválida la Decisión 2000/520/CE, con arreglo a la Directiva 95/46, sobre la adecuación de la protección basada por los principios de puerto seguro para la protección de la vida privada y en consecuencia, declaró inválidas las transferencias internacionales a los Estados Unidos con base en el Safe Harbor en tanto este esquema no ofrecía una protección adecuada de los datos personales.

Tiempo después, en diciembre de 2015, el Sr. Schrems modificó su reclamo y alegó, en particular, que conforme lo alegado por Facebook Ireland la transferencia de datos se

[69] Disponible en español en el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32000D0520&from=en

[70] Este acuerdo proponía un sistema de autocertificación mediante el cual si las empresas estadounidenses cumplían con ciertos requisitos obtenían una certificación que les permitía implementar las transferencias de datos de la Unión Europea a Estados Unidos bajo los principios de protección de datos europeos.

[71] Disponible en español en el siguiente enlace: https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=5796171

realizaba a EE.UU. basándose en las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión de la Comisión 2010/87/UE, de 5 de febrero de 2010[72], en su versión modificada por la Decisión de Ejecución (UE) 2016/2297 de la Comisión, de 16 de diciembre de 2016 (en adelante "Decisión 2010/87/UE") y que conforme la normativa estadounidense, la empresa Facebook Inc. se encuentra obligada a poner a disposición los datos personales que se le transfieren a las autoridades estadounidenses, tal como la "National Security Agency"[73] y la Federal Bureau of Investigation[74]. En virtud de ello, cuestionó la interpretación y la validez de la Decisión de la Comisión 2010/87/UE, y sostuvo que, la utilización de esos datos en el marco de diferentes programas de vigilancia violaba la Carta de los Derechos Fundamentales de la Unión Europea (en adelante la "Carta"). Específicamente, refiere a los artículos 7 (Respeto de la vida privada y familiar), 8 (Protección de datos de carácter personal) y 47 (Derecho a la tutela judicial efectiva y a un juez imparcial) y solicitó al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

En este escenario, el Comisario, inició un procedimiento ante el TJU. Vale aclarar que tras el inicio de este procedimiento, la Comisión, ante la imperiosa necesidad de establecer un nuevo mecanismo para legitimar las transferencias internacionales de datos hacia los Estados Unidos, adoptó la Decisión de Ejecución (UE) 2016/1250, de 12 de julio de 2016, con arreglo a la Directiva 95/46 sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU.[75], un acuerdo entre Estados Unidos y la Unión Europea. Las características principales de este acuerdo eran las siguientes: (i) imponía la obligación de adherirse al programa de certificación dispuesto por el propio acuerdo y obligaba a las empresas a contar con una política de privacidad acorde con los Principios de privacidad

[72] Relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46.
[73] En español "Agencia de Seguridad Nacional".
[74] En español "Oficina Federal de Investigaciones".
[75] Disponible en español el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=ES

(también determinados por el propio acuerdo), (ii) sumó nuevas obligaciones y estándares más exigentes para el intercambio internacional de datos personales y (iii) brindó herramientas a los ciudadanos europeos para resguardar sus derechos en caso de considerar que sus datos se hayan utilizado indebidamente[76].

ii. Planteamiento de las cuestiones prejudiciales y sentencia del TJUE

En mayo del año 2016, el Comisario para la Protección de Datos, Irlanda compartió las conclusiones provisionales de su investigación y declaró con carácter provisional que los datos personales de ciudadanos de la Unión Europea que sean transferidos a los Estados Unidos podrían ser objeto de consulta y ser tratados por las autoridades estadounidenses de forma incompatible con los artículos 7, 8 y 47 de la Carta.

En esas condiciones, mediante resolución de 4 de mayo de 2018, el Tribunal Superior de Irlanda planteó al Tribunal de Justicia la interpretación de las disposiciones que validan las transferencias internacionales a la luz de la Decisión 2010/87, sobre las cláusulas contractuales tipo y del Escudo de la Privacidad UE EE. UU. Asimismo, adjuntó una sentencia de la cual surgía que las actividades de inteligencia de las autoridades estadounidenses en lo que concierne a los datos personales transferidos a los Estados Unidos se basan, en particular, en el artículo 702 de la Foreign Intelligence Surveillance Act (FISA)[77], que permite a las autoridades estadounidenses la vigilancia de personas no nacionales de los Estados Unidos que se encuentren fuera del territorio de ese país y en la E.O. 12333 que habilita a la Agencia de Seguridad Nacional estadounidense para obtener datos en tránsito antes de su llegada al territorio nacional.

[76] A través de la página web https://www.privacyshield.gov/welcome# se podía consultar el listado de todas las empresas adheridas al Escudo de Privacidad y de este modo también identificar cuáles son aquellas empresas que ya no cumplen con los estándares impuestos por el acuerdo y en consecuencia ya no forman más parte.

[77] En español "Ley de Vigilancia de la Inteligencia Extranjera".

Basándose en las apreciaciones descriptas, el Tribunal Superior de Irlanda consideró que Estados Unidos lleva a cabo un tratamiento de datos masivo, sin asegurar una protección acorde a la garantizada por los artículos 7 y 8 de la Carta. Asimismo, advirtió que el Derecho estadounidense no ofrece a los ciudadanos europeos recursos compatibles con el artículo 47 de la ya mencionada Carta resaltando además que los ciudadanos de la Unión no cuentan con los mismos recursos que los americanos conservan contra el tratamiento de datos personales por parte de las autoridades estadounidenses. En este escenario, plantea al Tribunal de Justicia determinadas cuestiones prejudiciales, las cuales son exhaustivamente analizadas por el TJU, conforme se expone a continuación:

a. Ámbito de aplicación del RGPD

En primer lugar, el Tribunal Superior de Irlanda solicita confirmar si dentro del ámbito de aplicación del RGPD se encuentra comprendida una transferencia de datos personales realizada por un operador económico a otro ubicado en un tercer país cuando en el transcurso de esa transferencia o tras ella, estos datos puedan ser tratados por las autoridades de ese tercer país con fines de seguridad.

El TJU se pronuncia sobre el ámbito de aplicación del RGPD (artículo 2, apartados 1 y 2) y clarifica que esta transferencia de datos se encuentra efectivamente alcanzada por el Reglamento, incluso cuando durante esa transferencia o luego de ella, esos datos puedan ser tratados por las autoridades del tercer país con fines de defensa, seguridad nacional y seguridad del Estado.

Para resolver de esta manera, el TJU analizó la definición de "tratamiento" prevista en el artículo 4 del RGPD[78] y sostuvo que no se hacen distinciones entre las operaciones ejecutadas dentro de la Unión con aquellas que estén relacionadas con un tercer país. Destacó además que el propio Reglamento en su capítulo V provee mecanismos para la transferencia

[78] El artículo 4 del RGPD incluye las definiciones del Reglamento.

internacional de datos. En virtud de los dos fundamentos expuestos, concluyó que el hecho de transferir datos personales desde un Estado miembro a otro tercer país ya constituye un tratamiento de datos personales.

Asimismo, revisó el artículo 2 del RGPD que regula el ámbito de aplicación material y determinó que en el caso bajo estudio no resultaban aplicables ninguna de las excepciones allí previstas que justifique excluir la aplicación de esta norma.

Por último también agregó que la Comisión en virtud de lo dispuesto por el artículo 45, apartado 2, letra a) del RGPD se encuentra facultada para revisar el nivel de protección garantizado por un tercer país, incluyendo específicamente la legislación pertinente y lo que respecta a "…*la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación*…", lo que significa que el acceso y tratamiento de datos por un país tercero con fines de seguridad pública, defensa y seguridad del Estado no compromete la aplicabilidad del RGPD.

b. Elementos a considerar para determinar el nivel de protección

En el marco de una transferencia de datos personales a un tercer país basada en cláusulas tipo de protección de datos, se requiere al Tribunal de Justicia que detalle cuales son los elementos que deben revisarse a fin de determinar si el nivel de protección resulta adecuado y si se encuentra garantizado en el contexto de tal transferencia.

En lo que respecta a las garantías adecuadas, los derechos exigibles y las acciones legales efectivas (artículo 46, apartado 1 y apartado 2, letra c) del RGPD), el TJU resaltó que los derechos de aquellas personas cuyos datos personales se envían a un tercer país sobre la base de cláusulas tipo de protección de datos cuentan con un nivel de protección semejante al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta. En este sentido, la evaluación del nivel de protección garantizado en el contexto de una

transferencia con estas características debe tomar en consideración específicamente: (a) las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el tercer país en cuestión, incluyendo también el acceso eventual de las autoridades públicas de ese tercer país a los datos personales y (b) los elementos pertinentes del sistema jurídico de dicho país[79].

c. Atribuciones de la autoridad de control competente

Se solicita la interpretación del artículo 58, apartado 2, letras f) y j), del RGPD[80] a fin de resolver si la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos determinada por la Comisión en caso de que esa autoridad de control crea que la protección de los datos transferidos dispuesta por el Derecho de la Unión no puede asegurarse.

Al respecto, el TJUE aclara que de acuerdo con el artículo 58, apartado 2, letras f) y j) del RGPD, excepto que exista una decisión de adecuación válidamente dispuesta por la Comisión Europea, la autoridad de control competente tiene como función primordial vigilar la aplicación del RGPD y controlar su cumplimiento. En virtud de lo expuesto, la autoridad de control se encuentra obligada a suspender o prohibir una transferencia de datos a un tercer país cuando esta se encuentre basada en cláusulas tipo de protección de datos adoptadas por la Comisión y la autoridad considere que dichas cláusulas no se cumplen o no pueden cumplirse en ese tercer país y, como consecuencia la protección exigida por el Derecho de la Unión, en particular, por los artículos 45 y 46 del mencionado Reglamento y por la Carta, no puedan garantizarse mediante otros medios. Ello siempre que el responsable o el encargado del

[79] De conformidad con el artículo 45, apartado 2 del RGPD "Transferencias basadas en una decisión de adecuación" desarrollado más arriba en el presente exposición.

[80] Este artículo detalla los poderes que conserva cada autoridad de control. El Apartado f) establece que la autoridad de control podrá: "*imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición*" mientras que el Apartado j) dispone que este podrá: "*ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización Internacional*".

tratamiento establecidos en la Unión no hubieran ya suspendido la transferencia o puesto fin a esta por sí mismos.

d. Validez de la Decisión 2010/87 sobre las cláusulas contractuales tipo

Se cuestiona, específicamente, si a la luz de los artículos 7, 8 y 47 de la Carta, la Decisión 2010/87 sobre las cláusulas contractuales tipo puede considerarse válida, si esta puede garantizar un nivel de protección adecuado de los datos personales transferidos a terceros países en virtud de que estas cláusulas no resultan obligatorias para las autoridades estatales del tercer país de que se trata y, por lo tanto, no pueden subsanar una eventual falta de protección adecuada.

En relación a ello, el TJUE concluyó que a la luz de los artículos 7, 8 y 47 de la Carta la Decisión 2010/87/UE es válida. Para así determinar, el TJU distinguió la decisión de adecuación y las cláusulas tipo de protección de datos.

Resaltó que en el primer caso, el objeto es determinar si un tercer país garantiza un nivel de protección adecuado y para ello se deberá analizar la legislación pertinente en materia de seguridad nacional y el acceso de las autoridades públicas a los datos personales de conformidad con lo establecido en el artículo 45, apartado 2 letra a) del RGPD. Por consiguiente, la misma normativa admite la posibilidad de que exista acceso a los datos personales por parte de las autoridades públicas de un tercer país y no impide por ello la transferencia. En tal caso, lo que exige el artículo mencionado, es que la Comisión revise la legislación pertinente del tercer país de modo de verificar si cuenta efectivamente con todas las garantías exigibles para considerar que existen un nivel adecuado de protección.

Por otro lado, cuando se trata de una decisión que adopta cláusulas tipo de protección de datos, tal como es el caso de la Decisión 2010/87/UE, la Comisión no tiene la obligación de revisar el nivel de protección garantizado por el tercer país ya que de acuerdo al artículo 46, apartado 1, del mencionado Reglamento, estará a cargo del responsable o al encargado del

tratamiento establecidos en la Unión ofrecer las garantías adecuadas. En el mismo sentido, dado el carácter contractual de las cláusulas tipo de protección de datos, estas no pueden obligar a las autoridades públicas de terceros países, por lo que también será tarea del responsable o encargado del tratamiento comprobar, en cada caso, si el tercer país garantiza una protección adecuada y alineada con el RGPD y, de ser necesario, estos deberán adoptar garantías adicionales para asegurar la protección exigida por el Reglamento interpretados a la luz de los artículos 7, 8 y 47 de la Carta.

Cabe aclarar, que en caso de que el responsable o el encargado del tratamiento no pueda adoptar las medidas adicionales necesarias para asegurar la protección, estos y, con carácter subsidiario, la autoridad de control, están obligados a suspender o poner fin a la transferencia de datos personales al tercer país en cuestión.

e. Validez del Escudo de la Privacidad UE-EE. UU

Por último, el TJUE también examinó y resolvió que la Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE. UU. (conocida como "Privacy Shield") es inválida.

Para así concluir, el TJU sostuvo que de acuerdo a los lineamientos previstos por el artículo 45, apartado 3, del RGPD, la Comisión debió revisar las limitaciones y garantías establecidas por la normativa de los Estados Unidos. En particular, el artículo 702 de la FISA[81], la E.O. 12333[82], y la Directiva de Política Presidencial 28 (PPD-28)[83] en lo relativo al acceso a los datos personales transferidos en el marco del Escudo de la Privacidad UE-EE. UU. e

[81] Este artículo habilita al fiscal general y al director de los Servicios de Inteligencia Nacionales permitir la vigilancia de personas no nacionales de los Estados Unidos que se encuentren fuera del territorio de ese país a fin de adquirir información sobre inteligencia exterior.
[82] Orden Ejecutiva 12333que autoriza al gobierno para recopilar información esencial para la seguridad nacional de Estados Unidos.
[83] La PPD-28 son las políticas y los procedimientos que rigen la protección por parte de los empleados de la Oficina de Inteligencia y Análisis de la información personal recopilada de las actividades de inteligencia de señales.

investigar el uso de esos datos por las autoridades públicas para fines de seguridad nacional. Ello, a fin de asegurarse el cumplimiento de las garantías y derechos establecidos en los artículos 7,8 y 47 de la Carta.

Al respecto, cabe aclarar que de acuerdo con la Carta solo podrán introducirse limitaciones a los derechos y libertades allí garantizadas cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás[84]. A fin de cumplir con el principio de proporcionalidad se debe establecer de manera clara dicha limitación y determinar reglas precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas que permitan proteger los datos personales contra los riesgos de abuso.

Sobre esta base el TJU revisa el caso en autos y señala que: (i) no se garantiza un nivel adecuado de protección conforme lo establecido el artículo 45, apartado 2, letra a) del RGPD[85], en tanto el Gobierno estadounidense ha admitido que la PPD-28 no confiere a los titulares de los datos efectivos y exigibles ante los tribunales; (ii) el principio de proporcionalidad[86] no se encuentra garantizado en tanto los programas de vigilancia basados en los artículos 702 de la FISA y en la E.O. 12333 proceden con una recopilación "en bloque" sin que exista un criterio de selección específico para que se ejecute dicha recopilación y por lo tanto no se limitan a lo estrictamente necesario. Asimismo tampoco existe un control judicial; (iii) no se respeta el derecho a la tutela judicial efectiva independiente e imparcial garantizado por el artículo 47 la Carta[87] y resalta que la existencia del mecanismo del Defensor del Pueblo establecido por las

[84] Artículo 52: "Alcance de los derechos garantizados" de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01).
[85] Este artículo establece el requisito de que existan derechos efectivos y exigibles por parte del titular de los datos personales.
[86] El cual dispone que base legal que permita injerencias en los derechos fundamentales, debe establecer el alcance de la limitación del ejercicio del derecho de que se trate y determinar reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas
[87] Este artículo reza lo siguiente: "*Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída*

autoridades estadounidenses no suple esa falta en tanto no proporciona ninguna vía de recurso ante un órgano que ofrezca a las personas cuyos datos se transfieren a los Estados Unidos garantías sustancialmente equivalentes a las exigidas en el artículo 47 de la Carta.

Como consecuencia de la sentencia descripta, la cual anula la Decisión que establecía la validez del Escudo de la Privacidad UE EE. UU, las transferencias entre la Unión Europea y EE. UU. basadas en una decisión de adecuación ya no serán válidas, en tanto Estados Unidos ya no será considerado un país apto que cuente con garantías adecuadas.

Habiendo revisado la legislación europea en materia de protección de datos personales y luego de haber examinado su correspondiente aplicación, se observa, en primer lugar, la importancia y el valor que tiene el concepto de intimidad en la normativa europea. El reconocimiento del respeto a la vida privada y la protección de los datos de carácter personal como derechos fundamentales y, la tendencia de respetar estrictamente estos principios en la práctica hacen que el sistema normativo europeo resulte ejemplar a nivel internacional. Tal como surge del análisis del caso Schrems II, este elevado estándar de privacidad y seguridad de datos propuesto por la legislación de la Unión Europea no siempre se encuentra alineado con las exigencias de las legislaciones comparadas ya que, tal como sucede con la normativa norteamericana, el concepto de privacidad resulta más limitado y no tiene el mismo valor atento que la protección de datos no cuenta con el reconocimiento y status de derecho fundamental.

Asimismo, observamos que el RGPD contiene una regulación que se supo adaptar a las tecnologías actuales y que considera la importancia de regular el tráfico de datos. En este sentido, el Reglamento propone un renovado y diversificado conjunto de instrumentos de transferencia internacional[88]. Ello resulta manifiesto también en los fundamentos del TJU en

equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar…".

[88] Conforme surge de la Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el Intercambio y protección de los datos personales en un mundo globalizado, COM (2017) 7 final/2. Disponible en español el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007R(01)&from=ES

el caso Schrems II, donde se observa que el tribunal analiza las distintas herramientas propuestas por la normativa europea para el tráfico de datos y concluye que uno de los instrumentos utilizados para validar las transferencias entre Estados Unidos y Europa no ofrece una protección adecuada. Sin embargo, cabe señalar que esta sentencia no supone la creación de un vacío legal en tanto el propio Reglamento propone otros mecanismos para amparar las transferencias internacionales. En virtud de ello, aquellas empresas, organismos públicos y privados y, organizaciones internacionales que deseen ejecutar transferencias internacionales de datos entre los Estados Unidos y la UE, deberán repensar el marco jurídico para el flujo de datos y revisar cada una de las alternativas propuestas por el RGPD de modo de adoptar los lineamientos allí previstos a fin de validar las transferencias internacionales de datos.

En tercer lugar, cabe resaltar que la normativa europea propone un protección integral de los datos ofreciendo a todas las personas físicas de todos los Estados miembros el mismo nivel de derechos, incluyendo aquí no solo los derechos de acceso, rectificación, supresión, confidencialidad o actualización tal como sucede en los marcos normativos del derecho comparado[89], sino que además se compromete a proteger el derecho a la limitación del tratamiento[90], a la portabilidad[91], a la oposición del tratamiento y a no ser objeto de una decisión basada únicamente en el tratamiento automatizado[92] e impone la obligación de notificar los incidentes de seguridad[93]. Además, propone una protección de datos con vocación de universalidad[94], ya que conforme surge del Reglamento analizado y del caso Schrems II, todos los derechos y garantías previstos por el RGPD deben ser asegurados no solo dentro de la UE sino también en terceros territorios. Ello en virtud de que la normativa europea en materia de

[89] Por ejemplo como ocurre en la Ley de Protección de Datos Personales N.º 25.326. en su artículo 33.
[90] Conforme artículo 18 del RGPD.
[91] Conforme artículo 20 del RGPD.
[92] Conforme artículos 21 y 22 del RGPD.
[93] Conforme artículo 34 del RGPD.
[94] Cordero Álvarez, Clara Isabel (2019): "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: especial referencia al caso estadounidense y la Cloud Act", Revista Española de Derecho Europeo, 70, pp. 49-108.

protección de datos tiene un impacto potencial en cualquier empresa del mundo que realice tratamiento de datos de residentes de la UE u ofrezca bienes o servicios a residentes de la UE. Esta extraterritorialidad permite asegurar que, cuando se transfieran datos personales de ciudadanos europeos a terceros países, se mantenga el mismo nivel de protección y de este modo, que los titulares de los datos personales gocen de un nivel adecuado de protección de datos independientemente de las jurisdicciones que se encuentren involucradas. No obstante, tal como surge del análisis del caso Schrems II, la aplicación de este principio de extraterritorialidad puede resultar un desafío atento que a veces resulta incompatible y difícil de aplicar con algunas legislaciones comparadas, tal como sucede con Estados Unidos, cuya regulación no impone un marco normativo único aplicable a toda la jurisdicción norteamericana y cuyo enfoque se caracteriza por la privacidad sectorial/territorial y por establecer reglas específicas[95].

En cuarto lugar, se observa del Reglamento y del caso Schrems II, que la normativa europea propone un marco de protección de unificado y simplificado ya que armoniza los estándares que deben mantener las legislaciones locales vigentes de cada país. Ello genera la aplicación del mecanismo de "ventanilla única", lo que significa que una sola autoridad de protección de datos vigilará y velará por las operaciones transfronterizas de tratamiento de datos que las empresas y entidades públicas lleven a cabo en la Unión Europea. Además, asegurará una interpretación congruente de las nuevas normas. En especial, cuando se traten asuntos transfronterizos en los que intervengan diferentes autoridades nacionales de protección de datos, se adoptará una única resolución para garantizar que existan soluciones comunes a dilemas comunes[96].

[95] Schweighofer Erich (2017): "Trans-Atlantic Data Privacy Relations as a Challenge for Democracy", Publicado en Intersentia pp. 27 – 48. DOI: https://doi.org/10.1017/9781780685786.004.

[96] Conforme Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el Intercambio y protección de los datos personales en un mundo globalizado, COM (2017) 7 final/2. Disponible en español el siguiente enlace: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007R(01)&from=ES

Por último, resulta relevante agregar que el Reglamento provee un régimen sancionatorio equivalente en todos los Estados miembros, el cual resulta ejemplar a nivel mundial debido a las importantes multas administrativas involucradas generando un gran incentivo para el cumplimiento de la norma.

En virtud de las características descriptas y del caso analizado que demuestra el alto nivel de protección que ofrece a los ciudadanos europeos el RGPD[97], se concluye que el marco normativo europeo está a la vanguardia en materia de protección de datos en tanto reconoce el derecho a la privacidad como derecho fundamental, propone un sistema regulatorio transparente con reglas claras adaptado a los avances tecnológicos actuales, brinda seguridad jurídica integral a los titulares de los datos dentro y fuera de la Unión Europea, provee un régimen legal sólido mediante la imposición de obligaciones y garantías y, provee además un control judicial eficiente.

VI. Legislación argentina en materia de protección de datos personales

La legislación argentina también cuenta con un amplio marco normativo para legislar sobre la protección de datos personales. A continuación se detallarán brevemente los instrumentos locales e internacionales que conforman el marco regulatorio argentino en materia de protección de datos indicados en la Figura 3[98].

[97] Fuentes Máiquez, A. (2021). Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II). Icade. Revista De La Facultad De Derecho, (110), 1-10. https://doi.org/10.14422/icade.i110.y2020.009.

[98] Principales instrumentos legislativos para la protección de datos personales en Argentina.

i. Constitución Nacional Argentina

En la regulación argentina la protección de los datos personales se encontraba implícitamente garantizada en la Constitución Nacional en el artículo 18, el cual determinaba la inviolabilidad del domicilio, la correspondencia y los papeles privados, y en el artículo 19 el cual establecía el derecho a la privacidad. Tras la reforma del año 1994, esta protección fue ya explícitamente garantizada al incluir la acción de "Habeas Data"[99].

ii. Ley de Protección de Datos Personales N.º 25.326

Tiempo después, en el año 2000 y a fin de garantizar y fortalecer la protección de los datos personales se aprueba la Ley de Protección de Datos Personales N.º 25.326[100] (en adelante "LPDP"). Esta ley tiene específicamente como objeto garantizar la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes.

[99] Artículo 43, tercer párrafo de la Constitución Nacional. Se trata de un acción que toda persona podrá interponer para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.
[100] Disponible en el siguiente enlace: PROTECCION DE LOS DATOS (infoleg.gob.ar)

Esta ley define a los "datos personales" como cualquier información referida a personas físicas o de existencia ideal determinadas o determinables.

La semejanza de esta norma con el modelo europeo de protección de datos se hizo principalmente con el propósito de favorecer la transferencia de datos desde Europa, actividad esencial de la industria de tratamiento y requisito fundamental por su carácter transnacional[101]. De este modo, tal como se ha mencionado, Argentina fue considerada en el año 2003, como país adecuado para el tratamiento de datos personales de conformidad con el estándar europeo[102].

iii. Decreto N.º 1558/2001

En el año 2001 la LPDP fue reglamentada por el Decreto N.º 1558/2001[103] , modificado luego por el Decreto N.º 1160/2010[104], el cual creó la autoridad de aplicación: la Dirección Nacional de Protección de Datos Personales (en adelante "DNPDP") actualmente reemplazada por la Agencia de Acceso a la Información Pública[105], la cual tiene como misión principal garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover medidas de transparencia activa, y dictar normas y reglamentaciones en materia de protección de datos personales[106].

[101] Faliero, Johanna C. (2018), "El futuro de la regulación en protección de datos personales en la Argentina", Publicado en: Sup. Esp. LegalTech 2018 (noviembre), 05/11/2018, 55 Cita: TR LALEY AR/DOC/2375/2018.
[102] Conforme "Decisión de la Comisión del 30/06/2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina. Por favor ver nota al pie N.º 46.
[103] Disponible en el siguiente enlace: http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70368/norma.htm
[104] Disponible en el siguiente enlace: Decreto 1160/2010 (infoleg.gob.ar)
[105] Ente autárquico que funciona con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros del Poder Ejecutivo Nacional conforme la Ley N.º 27.275 de Acceso a la Información Pública
[106] Por ejemplo normas registrales, régimen sancionatorio, regulaciones especiales, normas de inspección y control, guías de buenas prácticas, organización interna, entre otras.

iv. Ley de Acceso a la Información Pública N.º 27.275

En el año 2016 se aprobó la Ley N.º 27.275 de Acceso a la Información Pública[107] a fin de regular la información que se encuentra en control del Estado y establecer los procedimientos que se deben seguir para solicitar el acceso a la información pública.

v. Convenio 108

En el año 2017, Argentina se adhiere al Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, hito sumamente relevante para que Argentina siga siendo considerada un país adecuado en los términos del RGPD.

vi. Nuevo Proyecto de Ley de Protección de Datos Personales

En el año 2022, la Agencia de Acceso a la Información Pública inicia un proceso de debate a fin de reemplazar la LPDP, el cual culminó en noviembre del mismo año con la presentación del Nuevo Proyecto de Ley de Protección de Datos Personales[108] ante el Congreso de la Nación Argentina. Este proyecto conformado por 80 artículos tiene como propósito actualizar la ley vigente que cuenta con más de 20 años de antigüedad implementando una ley que se adapte al auge de la era digital y a las transformaciones tecnológicas. Para ello toma en consideración los estándares, recomendaciones y enseñanzas aprendidas a nivel regional (por ejemplo las legislaciones de Brasil y Ecuador y los proyectos de ley de Chile, Paraguay y Costa Rica) y, a nivel internacional (tal como el RGPD y el Convenio 108). Entre las principales modificaciones cabe destacar la inclusión de nuevas definiciones (ampliando los conceptos

[107] Disponible en el siguiente enlace:
InfoLEG - Ministerio de Justicia y Derechos Humanos - Argentina

[108] Durante el proceso se recibieron 173 opiniones, aportes y comentarios presentados por 123 participantes correspondientes a la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, sector privado y sector público nacional e internacional.
Disponible en el siguiente enlace:
https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_datos_personales_aaip.pdf

existentes), la inserción del principio de extraterritorialidad, la incorporación de ciertos principios y bases para el tratamiento de datos personales, la inclusión de reglas que estimulan el flujo transfronterizo de datos, la suma de obligaciones y derechos y, el incremento de los montos de las sanciones.

VII. Transferencias internacionales de datos: marco normativo de Argentina

A fin de comprender los distintos mecanismos para la transferencia internacional de datos dispuestos por la normativa argentina vigente, revisaremos brevemente el ámbito de aplicación material y territorial de la LPDP y, se señalarán las definiciones más relevantes. Esto nos permitirá identificar en qué supuestos la LPDP resulta aplicable.

En primer lugar resulta relevante identificar quienes son los sujetos comprendidos por la LPDP. Al respecto cabe aclarar que esta norma no abarca solamente a quienes comercializan bases de datos o quienes prestan servicios de información a terceros. Por el contrario, esta adopta un criterio amplio ya que tal como se ha adelantado, el artículo 1 dispone que la misma tiene por objeto la protección "*de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes*". Por su parte, el Decreto Reglamentario 1558/2001, determinó que "*quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito*"[109]. Al respecto la doctrina ha interpretado que siempre que una persona transfiera a otra datos (distintos de los propios) se considerará que tales datos "exceden el uso personal" y en

[109] Conforme artículo 1 del Decreto Reglamentario N.°1558/2001.

consecuencia, se encuentran amparados por la LPDP, quedando tanto cedente como cesionario sujetos a cumplir sus disposiciones[110].

En virtud de lo expuesto, los principales destinatarios de la LPDP son: (i) el responsable de un archivo o base de datos[111], (ii) el usuario de datos[112] y, ante la transferencia de los datos, (iii) el cesionario de los datos recibidos (que queda solidariamente obligado con el cedente responsable de los datos por las obligaciones de la LPDP)[113] y por último, (iv) el titular de los datos objeto de tratamiento[114].

En lo que respecta al alcance territorial, la LPDP establece el principio de territorialidad, determinando que sus disposiciones aplican en todo el ámbito de la República Argentina[115].

[110] Frene, Lisandro (2006), "Transferencia de datos personales", Publicado en: LA LEY 28/04/2006, 1 - LA LEY2006-C, 1019 Cita: TR LALEY AR/DOC/1214/2006.

[111] Conforme el artículo 2 de la LPDP se entenderá por "Responsable de archivo, registro, base o banco de datos" como la "*Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos*".

[112] Conforme el artículo 2 de la LPDP se entenderá por "Usuario de datos" a "*Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos*".

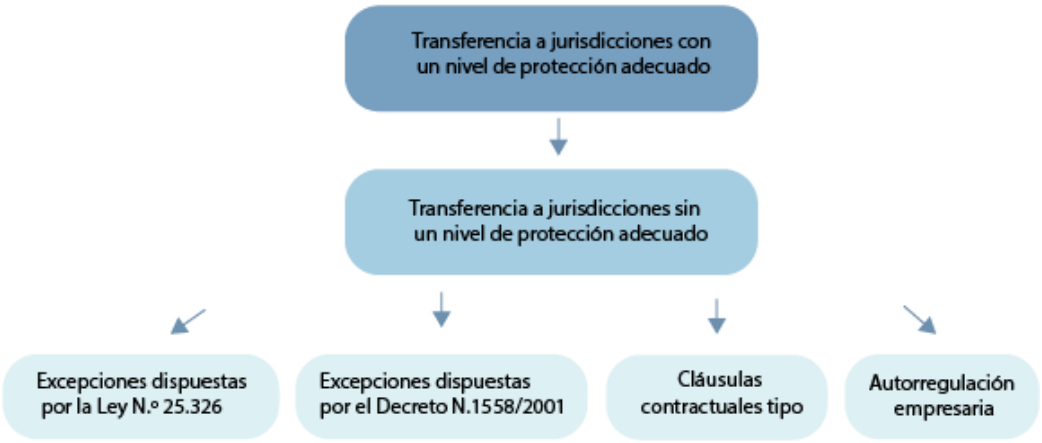
[113] Conforme el artículo 11, inciso 4 de la LPDP, el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

[114] Conforme el artículo 2 de la LPDP se entenderá por "Usuario de datos" como "*Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos*".

[115] El artículo 44 de la LPDP que refiere al ámbito de aplicación dispone que: "*Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional*."

A continuación describiremos los distintos mecanismos establecidos por la legislación local argentina para las transferencias internacionales de datos indicados en la Figura 4[116].

Mecanismos para transferencias internacionales de datos de Argentina



i. Transferencias mediante excepciones dispuestas por la LPDP

La LPDP detalla los lineamientos para las transferencias internacionales de datos y dispone en su artículo 12 que se encuentra prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados, excepto cuando se trate de los siguientes casos: (a) colaboración judicial internacional; (b) intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica; (c) transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; (d) si la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; (e) cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

[116] Mecanismos para transferencias internacionales de datos de Argentina.

En la práctica esta norma posee un alcance muy extenso, ya que cualquier transferencia internacional de datos personales debe respetar los requisitos dispuestos por la LPDP y al mismo tiempo, las excepciones establecidas por el artículo 12 resultaban ser acotadas para la aplicación al sector privado. Al respecto, cabe agregar que las transferencias más usuales son aquellas ejecutadas por sucursales/ sociedades a su casa matriz o al accionista en el extranjero así como también a empresas ajenas al grupo empresario, como por ejemplo a los proveedores. La razón detrás de estas transferencias es variada ya sea por ejemplo para unificar la visión global de una compañía sobre temas de ventas, o análisis de clientes, entre otros[117].

ii. Transferencias mediante excepciones dispuestas por el Decreto N.º 1558/2001

Las excepciones mencionadas en el punto anterior han sido ampliadas por el Decreto Reglamentario N.º 1558/2001, las cuales fueron incluidas siguiendo aquellas excepciones previstas en el artículo 26 de la Directiva Europea de Protección de Datos del año 1995[118], lo que significó una mayor alineación con la normativa europea. En este sentido, el artículo 12 dispone que también se permitirá la transferencia de datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados cuando el titular de los datos hubiera consentido expresamente esa cesión. Asimismo, se establece que no será necesario el consentimiento en caso de que se trate de una transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta. Por último, el Decreto faculta a la Dirección Nacional de Protección de Datos Personales a evaluar el nivel de protección

[117] Palazzi, Pablo A. (2017): "Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales", Publicado en: LA LEY 15/02/2017, 1 - LA LEY2017-A, 1039 Cita: TR LALEY AR/DOC/3904/2016.

[118] Este artículo dispone las excepciones a las transferencias de datos personales a terceros países.

proporcionado por las normas de un Estado u organismo internacional. Se considerará que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando la tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales.

Esta ampliación resultaba sumamente necesaria a fin de permitir que se desarrollen las transferencias en un mundo interconectado. De esta manera, el carácter rígido y limitado que presentaba la LPDP se flexibilizó. Por ejemplo mediante la inclusión de que el consentimiento del sujeto autorizaba las transferencias internacionales o mediante cláusulas contractuales. Al respecto, cabe aclarar que si bien el Decreto Reglamentario N.º 1558/2001 habilitaba a las partes a transferir datos de forma internacional a países no adecuados mediante contratos o cláusulas que aseguren una protección adecuadas, la autoridad regulatoria no aprobó un modelo oficial hasta la sanción de la Disposición E 60/2016 de la Dirección Nacional de Protección de Datos Personales[119] (tal como sucedía en Europa[120]). En virtud de ello, las partes acordaban los términos y condiciones para las transferencias sin que exista una guía como modelo. Sin embargo, cabe agregar al respecto que la DNPDP a pedido de parte podía revisar los proyectos de los acuerdos y emitir un dictamen sobre la adecuación del mismo. Estos dictámenes crearon jurisprudencia administrativa[121] que servía para entender los requisitos para dar base legal a una transferencia internacional de protección de datos personales a una jurisdicción no

[119] Disponible en el siguiente enlace: https://www.argentina.gob.ar/normativa/nacional/disposici%C3%B3n-60-2016-267922/actualizacion

[120] Acceso a más información en el siguiente enlace: Data protection | European Commission (europa.eu)

[121] Ver dictámenes de la DNPDP disponibles en http://www.jus.gob.ar/datos-personales/normativa/dictamenes-pdp.aspx

adecuada. Operativamente, en la realidad, las compañías utilizaban un modelo alineado con el aprobado en la Unión Europa[122].

iii. Cláusulas contractuales tipo

A fin de limitar los alcances de la LPDP, en el año 2016, la entonces DNPDP creó la Disposición 60/2016, a fin de "*garantizar un nivel adecuado de protección de datos personales en los términos del art. 12 de la ley 25.326 en aquellas transferencias de datos que tengan por destino países sin legislación adecuada*"[123]. La Disposición E 60/2016 de la Dirección Nacional de Protección de Datos Personales (en adelante la "Disposición E 60/2016") hizo lo siguiente: (i) aprobó las cláusulas contractuales tipo de transferencia internacional en aquellas transferencias de datos que tengan por destino países sin legislación adecuada, (ii) determinó la necesidad de requrir autorización para usar un modelo diferente al propuesto por la misma disposición y (iii) definió en su artículo 3 cuales son los países considerados como "adecuados"[124].

Cabe aclarar que las cláusulas contractuales tipo no serán necesarias si el país de destino tiene una legislación adecuada, en cuyo caso las partes conservan la libertad de acordar los términos y condiciones de la transferencia con un contrato de procesamiento de datos, de locación de servicios o uno genérico de outsourcing, siempre cumpliendo los requisitos del artículo de la LPDP y del Decreto Reglamentario N.º 1558/2001. Esto brindó fundamentos para

[122] Palazzi, Pablo A. (2017): "Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales", Publicado en: LA LEY 15/02/2017, 1 - LA LEY2017-A, 1039 Cita: TR LALEY AR/DOC/3904/2016.

[123] Conforme artículo 1.

[124] Este artículo 3 fue sustituido por artículo 1° de la Resolución N.º 34/2019 de la Agencia de Acceso a la Información Pública B.O. 26/02/2019. Al respecto dispone lo siguiente: "ARTÍCULO 1º: Sustitúyese el artículo 3 de la Disposición 60 - E/2016, el que quedará redactado conforme el siguiente texto: "*A los fines de la aplicación de la presente disposición, se consideran países con legislación adecuada, a los siguientes: Estados miembros de la UNIÓN EUROPEA y miembros del espacio económico europeo (EEE), REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE, CONFEDERACIÓN SUIZA, GUERNSEY, JERSEY, ISLA DE MAN, ISLAS FEROE, CANADÁ sólo respecto de su sector privado, PRINCIPADO DE ANDORRA, NUEVA ZELANDA, REPÚBLICA ORIENTAL DEL URUGUAY y ESTADO DE ISRAEL sólo respecto de los datos que reciban un tratamiento automatizado*".

considerar que la libertad de las partes de no usar contratos de transferencia se extiende a aquellos países de la UE (o reconocidos por tal Unión como adecuados), donde la legislación se encuentra alineada con la ley argentina[125].

iv. Autorregulación empresaria

A través de la Resolución N.º 159/2018 la Agencia de Acceso a la Información Pública[126] delineó los contenidos básicos de una autorregulación empresaria para ser considerada lícita y para que las normas de autorregulación protejan adecuadamente los datos personales que se transfieran a países sin legislación adecuada. Con este fin aprueba los "Lineamientos y Contenidos Básicos de Normas Corporativas Vinculantes" y dispone que en caso de que no respeten estos lineamientos propuestos, las empresas deberán presentar las normas ante la Agencia para su control y aprobación en un plazo de 30 días siguientes de efectuada la transferencia.

VIII. Unión Europea vs. Argentina

Tal como se observa en el desarrollo de esta exposición, la normativa de la Unión Europea y la regulación local argentina comparten lineamientos y principios similares. Sin embargo, al analizar más en detalle algunas de las características propias de ambos sistemas se observan ciertas diferencias que resultan relevantes para mantener un sistema normativo acorde al avance de las tecnologías de la información y, al mismo, asegurar un régimen jurídico transparente que garantice una protección adecuada de los datos personales que se transfieren en el marco del mundo globalizado actual. A continuación, analizaremos algunas de estas diferencias y desarrollaremos a partir de la normativa europea, por qué ciertos aspectos de la

[125] Palazzi, Pablo A. (2017): "Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales", Publicado en: LA LEY 15/02/2017, 1 - LA LEY2017-A, 1039 Cita: TR LALEY AR/DOC/3904/2016.
[126] Disponible en el siguiente enlace: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-159-2018-317228/texto

actual normativa local argentina en lo que respecta a la transferencia internacional de datos debieran desafiarse.

En primer lugar cabe analizar el ámbito de aplicación de la normativa. Tal como hemos detallado más arriba, la LPDP, conforme su artículo 44, se aplica en todo el ámbito de la República Argentina. Por su parte, el Decreto N.º 1558/2001 que reglamentó la LPDP no incluyó referencia alguna sobre el alcance territorial que suplemente o modifique la ley. Por lo tanto, se concluye que la normativa local argentina no se aplica extraterritorialmente al procesamiento de datos realizado fuera de las fronteras nacionales. Podría pensarse que la razón de ello se debe a que al momento en que se aprobó la LPDP el desarrollo tecnológico no contemplaba la conectividad actual. No obstante, es importante señalar que han existido distintos pronunciamientos de las autoridades locales y de los tribunales[127] que han entendido que era necesario extender el ámbito de aplicación de la ley a fin de alcanzar procesamientos de datos que no eran efectuados en Argentina pero que tenían efectos en el país[128].

En contraposición, tal como resulta de la normativa europea analizada, el Reglamento posee un alcance extraterritorial garantizando su efectiva aplicación fuera del ámbito de la Unión Europea protegiendo así los datos personales de los titulares independientemente de las jurisdicciones involucradas. Para ello, el RGPD impone un amplio y complejo catálogo de obligaciones que en la práctica generan la necesidad de revisar procedimientos, políticas y documentos internos. De esta manera se asegura entonces una protección alineada y adecuada con el Reglamento y se garantiza que los derechos de los titulares no se vean afectados.

Al respecto cabe agregar que del caso Schrems II, analizado en esta exposición, surge la importancia de la aplicación extraterritorial de la norma. Ello consideración de que, las

[127] Fallo de la Cámara Federal de Apelaciones de Mendoza, Sala B, en "P. A. E. c. Facebook Argentina SRL s/ medida autosatisfactiva", de fecha 24/05/2019, AR/JUR/12577/2019 y Resolución de la Agencia de Acceso a la Información Pública en el expediente "Giolito c. Google Argentina SRL y Google LLC - EX-2019-84609512 - APNDNPDP#AAIP RESOL-2020-69-APN-AAIP", de fecha 13/04/2020.
[128] Peruzzotti, Mariano (2020): "Alcance territorial de las Leyes de Protección de Datos Personales", Publicado en: LA LEY 19/11/2020 , 1 LA LEY 2020-F , 428Cita: TR LALEY AR/DOC/2634/2020.

distintas regulaciones que existen entre los diferentes países proponen estándares de exigencia desiguales, lo que puede provocar que en la práctica quede sin efectos la protección de datos exigida por la normativa local, como ocurre por ejemplo cuando estos datos se localicen en países con un nivel de protección baja. En virtud de lo expuesto, consideramos la LPDP también debiera reflejar este aspecto en sus disposiciones de modo de que esta ley también resulte aplicable fuera del territorio argentino. El alcance extraterritorial permitirá que siempre que exista una transferencia de datos se garantice una protección integral, asegurando que las transferencias no puedan ejecutarse violando los derechos de los usuarios y menoscabando el nivel de protección adecuado[129]. Asimismo, cabe agregar que la inclusión de esta disposición evitará que la aplicación del derecho local siga siendo una cuestión debatible y controversial que requiere la revisión y análisis de los reguladores y jueces para definir, según el caso concreto, la norma aplicable[130].

En segundo lugar, cabe analizar los elementos que se deben considerar para determinar que existe un nivel de protección adecuado. Tal como hemos detallado más arriba, el RGPD dispone que se encuentran permitidas las transferencias internacionales de datos a terceros países que proporcionen niveles de protección adecuados y para ello establece que la Comisión luego de revisar si el tercer país ofrece un nivel de protección de datos adecuado, emitirá una "Decisión de adecuación", creando de este modo una especie de "lista blanca". Para la aplicación de este mecanismo, la normativa europea facilita un catálogo preciso y detallado de los elementos que la Comisión debe tener en cuenta al evaluar la adecuación del nivel de protección previsto en el ordenamiento jurídico de un tercer país o de una organización internacional[131]. De esta manera la normativa europea brinda transparencia y al mismo tiempo

[129] Considerando 101 del RGPD.
[130] Peruzzotti, Mariano (2020): "Alcance territorial de las Leyes de Protección de Datos Personales", Publicado en: LA LEY 19/11/2020, 1 - LA LEY2020-F, 428 Cita: TR LALEY AR/DOC/2634/2020.
[131] Conforme Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el Intercambio y protección de los datos personales en un mundo globalizado, COM (2017) 7 final/2. Disponible en español el siguiente enlace:

asegura su uniformidad. Ello resulta también de los fundamentos del caso Schrems II, en tanto el TJU responde cuales son los elementos y aspectos del marco jurídico del tercer país que la Comisión debe analizar a fin de determinar si ese tercer país cuenta efectivamente con todas las garantías necesarias para considerar que existe un nivel adecuado de protección.

Por su parte, Argentina también permite la transferencia internacional de datos personales de cualquier tipo con países u organismos internacionales o supranacionales que proporcionen niveles de protección adecuados. Como se observa, la normativa local adoptó un sistema similar al europeo de "lista blanca" y se sumó a autorizar las transferencias que se ejecuten a países que sean considerados adecuados por la Unión Europea. De esta manera la agencia de protección de datos se "ahorra" el trabajo de analizar la adecuación de cada país. Sin embargo, a diferencia de la normativa europea, la LPDP omitió explicar en detalle cómo se determina que un país u organismo internacional es adecuado. Si bien el Decreto N.º 1558/2001 atenuó esta situación en tanto estableció ciertas pautas que permiten concluir cuándo un país es adecuado[132], consideramos que resulta necesario que la DNPDP ofrezca una mayor transparencia a este mecanismo y desarrolle un método claro que explique detalladamente como se concluye que un país ofrece un nivel adecuado de protección. Al respecto, la postura del Dr. Palazzi[133] resulta una propuesta interesante ya que plantea adoptar el método ideado por la Unión Europea el cual establece que todo análisis significativo de la protección adecuada debe comprender de dos elementos básicos: (i) el contenido de las normas

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007R(01)&from=ES

[132] De acuerdo con el artículo 12 de la LPDP se deberá revisar todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

[133] Conforme surge del siguiente articulo: Palazzi, Pablo A. (2017): "Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales", Publicado en: LA LEY 15/02/2017, 1 - LA LEY2017-A, 1039 Cita: TR LALEY AR/DOC/3904/2016.

aplicables, las cuales deben contar con determinados principios que se detallan a continuación y (ii) los medios para asegurar su aplicación eficaz[134].

En lo que respecta al contenido de las normas aplicables, este método sostiene que deben encontrarse incluidos los siguientes principios básicos: (i) Principio de limitación de objetivos (lo que implica que los datos sean objeto de tratamiento con un propósito determinado y que estos puedan transferirse siempre que ello resulte necesario y alineado con el propósito original); (ii) Principio de proporcionalidad y de calidad de los datos (lo que significa que los datos deben ser exactos y limitados con el objetivo específico que se traten); (iii) Principio de transparencia (lo que conlleva que el usuario se encuentre informado sobre el propósito y responsable del tratamiento); (iv) Principio de seguridad (lo que supone que los responsable del tratamiento deben tomar medidas adecuadas en función a los riesgos involucrados); (v) Derechos de acceso, rectificación y oposición (lo que implica que el interesado debe conservar estos derechos); (vi) Restricciones respecto a transferencias sucesivas a otros terceros países (lo que significa que las transferencias solamente puedan ejecutarse siempre que el país de destino cuente con un nivel de protección adecuado); (vii) Datos sensibles (lo que conlleva que ante tratamiento de datos sensibles deben sumarse medidas extra de protección); (viii) Mercadotecnia directa (supone que ante un caso de mercadotecnia directa, el interesado pueda oponerse a que sus datos sean tratados con esa intención) y (ix) Decisión individual automatizada (lo que implica que el interesado entienda la lógica detrás de ese proceso y debe contar con garantías adicionales para proteger sus intereses). Por otro lado, en lo que respecta a los "Mecanismos del procedimiento y de aplicación" establece que resulta esencial identificar los objetivos de un sistema normativo de protección de datos, y desde allí juzgar los diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países. Los

[134] Este método fue ideado por Grupo de Trabajo del Artículo 29, un grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta la entrada en vigor del RGPD.

objetivos de un sistema de protección de datos son esencialmente tres: (i) ofrecer un nivel satisfactorio de cumplimiento de las normas, (ii) ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos y (iii) ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas.

En tercer lugar, cabe revisar las atribuciones de la autoridad de control competente en el marco de las transferencias de datos. Conforme mencionamos anteriormente, ante la falta de una decisión de adecuación, los regímenes normativos europeos y argentinos establecen que las transferencias internacionales pueden, entre otros mecanismos, basarse en instrumentos alternativos de transferencia que ofrezcan garantías adecuadas en materia de protección de datos. Tal es el caso de las cláusulas contractuales tipo de transferencia internacional adoptadas por la Comisión o la DNPDP respectivamente.

Este mecanismo de transferencia de datos es analizado también en los fundamentos de la sentencia del caso Schrems II, mediante el cual el TJU revisó la implementación de la teoría normativa europea en la práctica, y concluye una observación importante que consideramos debiera ser adoptada en nuestro ordenamiento jurídico local. Específicamente, el TJUE concluye la validez de la utilización de las cláusulas contractuales modelo pero establece a cargo de las autoridades de aplicación de cada país y de los exportadores de los datos, la obligación de verificar caso por caso si la normativa de cada país de destino es susceptible de afectar los derechos de los titulares de los datos personales (en especial, ante eventuales accesos a los datos personales por autoridades públicas del país de destino), aun habiéndose implementado el contrato modelo de transferencia internacional. El fallo determina entonces que los contratos de transferencia internacional no deben ser utilizados como una protección y validación automática de la transferencia, debiendo las autoridades de aplicación locales prohibir las transferencias internacionales cuando determinen que las cláusulas contractuales no se podrán cumplir en el país de destino.

Por su parte, la normativa argentina copia esta herramienta del sistema europeo y bajo la Disposición E-60/2016 de la Dirección Nacional de Protección de Datos Personales, adopta la implementación de un contrato de transferencia internacional (incluyendo en su disposición el modelo que debe utilizarse) y de este modo permite automáticamente las transferencias internacionales a países que no presten protección adecuada, sin que se requiera en estos casos la autorización ni la intervención de la autoridad de aplicación. Sin embargo, conforme se ha demostrado en el caso Schrems II, aun cuando se utilicen los modelos propuestos por las autoridades de aplicación correspondientes, ello no implica necesariamente que se cumplen con los estándares adecuados de protección. En consecuencia, el uso de cláusulas tipo no excluye el deber de revisar si, a la luz del contexto que rodea la transferencia, las cláusulas tipo de protección de datos no se respetan o no pueden ser cumplidas en el país tercero al que los datos van a ser transferidos[135]. En virtud de lo descripto, consideramos que la LPDP debiera incluir dentro de sus disposiciones la intervención de la autoridad de aplicación incluso en los casos en que se aplique el contrato modelo propuesto por la propia normativa ello a fin de evitar que exista un grave riesgo de elusión y garantizar efectivamente una protección adecuada de los datos personales.

IX. Reflexiones finales

Tal como surge de los considerandos incluidos en el Reglamento, la magnitud de la recogida y del intercambio de datos personales ha aumentado significativamente y resultan fundamentales en el desarrollo de la economía mundial actual, por lo tanto restringir las transferencias internacionales de datos no resulta una buena estrategia atento que ello perjudicaría la economía nacional y el comercio electrónico. A fin de proteger adecuadamente

[135] De Miguel, Pedro Alberto (2020): "Implicaciones de la declaración de invalidez del Escudo de Privacidad", Publicado en: La Ley Unión Europea, Número 84 (septiembre 2020), https://eprints.ucm.es/id/eprint/62504/1/PADemiguelAsensio%20LaLey%20UE%20n%2084%2009.20.pdf.

este gran caudal de transferencias de datos personales e impedir las vulneraciones al derecho a la privacidad se requiere de un marco jurídico coherente que sea respaldado por una ejecución estricta. Si bien Argentina cuenta con un marco normativo de protección de datos sólido, consideramos que existen ciertos aspectos que deben ser revisados y actualizados a fin de reforzar su seguridad jurídica y transparencia. Para ello, entendemos que la normativa local argentina debiera adoptar las tendencias internacionales en el derecho comparado, especialmente aquellas impuestas por el RGPD.

En primer lugar, contar con un régimen de aplicación extraterritorial facilitará la libre circulación de datos personales y al mismo tiempo, garantizará un elevado nivel de protección resguardando los datos y derechos de los ciudadanos incluso fuera de los límites territoriales locales. Este aspecto resulta esencial ya que, tal como observamos del caso Schrems II, los estándares de protección propuestos por el derecho comparado no siempre se encuentran alineados con la normativa local. Al mismo tiempo, la inclusión de la extraterritorialidad en la ley argentina permitirá que la aplicación de la norma no se encuentre sujeta a la interpretación de los jueces garantizando de este modo una protección efectiva e integral de los datos personales.

En segundo lugar, la inclusión precisa de los elementos que se deben evaluar para concluir si un país o una organización ofrece un nivel adecuado de protección brindará a la normativa local argentina un proceso de evaluación más transparente y permitirá determinar de manera más clara si los estándares de protección propuestos por la ley argentina se encuentran reflejados en la ley extranjera. La normativa europea resulta útil en este aspecto, atento que, tal como surge del caso Schrems II, el RGPD incluye en su normativa un detalle claro sobre cuáles son los elementos que la Comisión Europea debe revisar para determinar cómo es el nivel de protección de datos que ofrece un país o una organización.

En tercer lugar, la intervención de la autoridad de aplicación a fin de controlar el adecuado cumplimiento de la normativa resulta esencial. La importancia de esta incorporación se manifiesta en el caso Schrems II, en tanto la autoridad de aplicación actúa como un supervisor externo que revisa el cumplimiento de la ley. Esta enmienda a la LPDP no solo evitaría el riesgo de elusión de la ley sino que también ayudaría a fortalecer la confianza de los titulares de los datos en lo que respecta a la seguridad de su información.

A modo de colofón, concluimos que modificar la normativa argentina para adoptar los estándares de protección europeos resulta una medida necesaria y favorable para los usuarios a nivel individual y colectivo. A nivel individual, estos verán fortalecida la protección de sus datos personales incluso fuera de las fronteras nacionales y tendrán mayores garantías para asegurar sus derechos. Estos beneficios individuales, tendrán un efecto a nivel colectivo, ya que si los usuarios confían en que sus datos se encuentran debidamente protegidos estos estarán dispuestos a compartir su información personal estimulando así el crecimiento del comercio electrónico y la inversión extranjera. Además, alinear la normativa local con la regulación europea, fortalecerá aún más la posición de Argentina para atraer inversión extranjera debido que las empresas foráneas ahorrarán costos para dar cumplimiento a su normativa local y evitarán asumir el riesgo de estar sujetos a potenciales sanciones y multas en su país de origen.

X. Bibliografía

Abdelnabe Vila, María C. - Cisilino, Arnaldo (2020): "Perspectivas de la Protección de Datos Personales: status quo y proyecciones", Publicado en: SupAbCorp 2020 (noviembre), 27/11/2020, 1 Cita: TR LALEY AR/DOC/3772/2020.

Andoni Polo Roca (2021): "Las transferencias internacionales de datos: regulación actual y su incidencia en las relaciones exteriores de la Unión Europea". Publicado en: Revista Aragonesa de Administración Pública ISSN 2341-2135, núm. 57, Zaragoza, 2021, pp. 325-369.

Basavilbaso, Marina (2022): "Régimen argentino de protección de datos personales", Publicado en: RCCyC 2022 (abril), 05/04/2022, 5 Cita: TR LALEY AR/DOC/771/2022.

Cordero Álvarez, Clara Isabel (2019): "La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: especial referencia al caso estadounidense y la Cloud Act", Revista Española de Derecho Europeo, 70, pp. 49-108.

De Miguel, Pedro Alberto (2020): "Implicaciones de la declaración de invalidez del Escudo de Privacidad", Publicado en: La Ley Unión Europea, Número 84 (septiembre 2020), https://eprints.ucm.es/id/eprint/62504/1/PADemiguelAsensio%20LaLey%20UE%20n%2084%2009.20.pdf

Faliero, Johanna C. (2018), "El futuro de la regulación en protección de datos personales en la Argentina", Publicado en: Sup. Esp. LegalTech 2018 (noviembre), 05/11/2018, 55 Cita: TR LALEY AR/DOC/2375/2018.

Frene, Lisandro (2006), "Transferencia de datos personales", Publicado en: LA LEY 28/04/2006, 1 - LA LEY2006-C, 1019 Cita: TR LALEY AR/DOC/1214/2006.

Frene, Lisandro (2018): “Reglamento General de Protección de Datos de la Unión Europea. Extraterritorialidad e impacto en Argentina”, Publicado en: LA LEY 06/09/2018, 1 – LA LEY2018-E, 1275 Cita: TR LALEY AR/DOC/1764/2018.

Fuentes Máiquez, A. (2021). “Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II)”. Publicado en: Icade. Revista De La Facultad De Derecho, (110), 1-10. https://doi.org/10.14422/icade.i110.y2020.009.

Guini, Leonor (2020): “Guía de Evaluación de Impacto en la protección de datos”, Publicado en: SJA 08/07/2020, 87 - Cita: TR LALEY AR/DOC/1977/2020.

Michaels, Ralf (2006), “The Functional Method of Comparative Law”, Publicado en: The Oxford Handbook of Comparative Law, Paper No. 87. Disponible en inglés en el siguiente enlace: SSRN: https://ssrn.com/abstract=839826.

Miller, Jonathan M. (2006), “Una tipología de los trasplantes legales: utilizando la sociología, la historia del derecho y ejemplos argentinos para explicar el proceso de trasplante”, Publicado en Lecciones y ensayos Nº 81, Disponible en español el siguiente enlace: http://www.derecho.uba.ar/publicaciones/lye/revistas/81/una-tipologia-de-los-transplantes-legales.pdf.

Sobrino García, I. (2021): “Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos”, Revista de Derecho Comunitario Europeo, 68, 227-256. doi: https://doi.org/10.18042/cepc/rdce.68.07.

Trevisán, Pablo (2022): “Competencia, datos y economía digital”, Publicado en: LA LEY 20/09/2022 , 1, Cita: TR LALEY AR/DOC/2726/2022.

Palazzi, Pablo A. (2017): "Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales", Publicado en: LA LEY 15/02/2017, 1 - LA LEY2017-A, 1039 Cita: TR LALEY AR/DOC/3904/2016.

Peruzzotti, Mariano (2020): "Alcance territorial de las Leyes de Protección de Datos Personales", Publicado en: LA LEY 19/11/2020, 1 - LA LEY2020-F, 428 Cita: TR LALEY AR/DOC/2634/2020.

Peruzzotti, Mariano (2022): "Reflexiones acerca de la política de protección de datos personales del ReNaPer", Publicado en: LA LEY 22/03/2022, 1 Cita: TR LALEY AR/DOC/1025/2022.

Schweighofer, Erich (2017): "Trans-Atlantic Data Privacy Relations as a Challenge for Democracy", Publicado en Intersentia pp. 27 – 48. DOI: https://doi.org/10.1017/9781780685786.004.

Velázquez, Jorge D. (2019): "Protección de datos: Una nueva era en la cultura de la privacidad" Publicado en: SJA 03/04/2019, 53 - Cita: TR LALEY AR/DOC/1170/2019.

Weber, Rolf H. (2017): "Transnational Data Privacy in the EU Digital Single Market Strategy", Publicado en Privacy and Transborder Flows of Personal Data, pp. 5 – 26, Cambridge University Press.